信息安全与“三金工程”

Information Security and China's Information Engineering

赵战生
（中国科学技术大学研究生院信息安全国家重点实验室，教授　　北京　100039）

一、“三金工程”可能受到的信息安全威胁

由金桥、金关、金卡组成的三金工程是促进我国信息化的国家重点工程。金桥的重点是解决信息传递交换的信道联网，它将把空中的卫星、无线传输、微波传输与地面的有线交换和光纤传输全面组织起来，提供信息国道。已初步建立的邮电通信系统、国家经济信息系统、银行业务管理系统、铁路运营系统、民航旅客服务计算机系统、电网监控系统、天气预报系统、科技情报信息系统、公安信息系统、财税系统、物资管理系统、国家统计系统等 12 个信息系统都将结合在金桥上。金关的重点是解决海关报关的信息化、自动化，它将以电子数据交换(EDI)的方式与国际标准接口，也将促进国内的无纸办公的发展。金卡将使我国的支付手段跨上一个新台阶，必将促进我国的银行金融与商业领域的电子化、信息化、自动化，减少现金流通，加速资金流动，提高服务效率与质量。

“三金工程”构作起来的信息系统必将会参照国际标准化组织(ISO)制定的开放系统互连(OSI)的相应标准协议，将会把国际上已成功应用的分组交换的 CCITT、X.25 推荐标准以及适用于公用交换数据网 PSDN 的 X.32 推荐标准和适应国际电子信息交换的信息处理系统(MHS)的 X.400 推荐标准、电子数据交换 EDI 标准等应用于系统之中，形成一个开放互连的分布式大系统。

仅就此系统的信息安全而论，将会面临来自用户或某些程序的如下威胁：

1. 冒充(Masquerade)　它来自某些非法实体成功地假冒一个合法实体，可能产生于非法实体假冒或盗用合法实体的身份证明；成功地攻击使用合法实体的签名进程；伪造了合法实体的安全参数；假冒某个合法实体的管理者身份；假冒其他网络的一个合法网络用户等。

2. 非法合作(Illegal Associations)　如果一个入侵者突破系统身份鉴别及访问控制的防线获得确认，违背安全规则，改变鉴别信息与授权管理，就将建立起网络实体与资源间的非法逻辑关系。

3. 非授权访问(Non－Authorized Access)　入侵者(可能是一个合法用户，但在进行非法操作)成功地全面违背访问控制服务(可能进行了修改控制文件的内容)，从而进行超出安全规定的操作行为。

4. 拒绝服务(Denial of Service)　系统拒绝一个合法网络用户执行他的功能。可能表现为拒绝访问、拒绝信息传输、故意抑制发给特写用户的信息或另发其他信息。

5. 否认(Repudiation)　产生于某些网络用户欺骗性地拒绝任务提交，拒绝接收消息，拒绝分担合作。可能表现为源否认、传递否认、提交否认、行为否认等。

6. 信息泄漏(Leakage of Information)　可能产生于传送中的或数据库中在存储中的信息被未授权者访问而泄密；可能造成隐匿的身份被暴露；可能使网、库中的信息资源被盗用。也可能由于信源端的电磁辐射而泄漏敏感信息。

7. 业务分析(Traffic Analysis)　当敌手面对保密处理的信息无法理解时，他可能转而通过获取协议控制信息、信息长度、频度、传输信息的源与目的地址来分析业务状况，从中获得所需信息。

8. 非法的消息顺序(Invalid message Sequencing)　用非法修改、删除、重排序、重放等手段，使正常传送的消息乱序。

9. 数据修改或破坏(Data Modification or Destruction)　有意无意地修改或删除了通信信息或数据库中的数据或程序，或删除信息中的敏感段(标号、属性、接收地址、原始识别符等)，或合法信息数据或程序的某些部分被随机修改。

10. 信息推理(Deduction of Information)　利用经过安全保护的数据库中公开发布的公用概要

(如统计数据)的数据项、借助概要中包含的原始信息痕迹,用信息论的演绎推理、统计方法、数学方法与公式等分析方法,经过推理获得信息。

11. 程序非法修改(Illegal Modification of Programs) 存于库中的操作系统模块、通信软件或用户的应用软件被计算机病毒、特洛伊木马、蠕虫等非法修改。

以上种种威胁轻则造成局部操作失败,重则造成整个系统瘫痪,如经济金融、银行支撑管理的信息系统的安全受损,将会损失大量钱财。从某种意义上讲,对现代信息系统的严重破坏所造成的损失绝不轻于核战争。因此,没有信息安全保护的信息系统是一个不完备的信息系统,信息系统的共享程度越高,信息安全的保障措施就越困难,越必要。我们绝不可掉以轻心。

二、信息安全的内涵

信息安全(Information Security)的内涵经过学术界的研究,已日益丰富起来并逐渐取得共识。通常大家认为主要应该包含如下方面:

1. 信息的机密性(Confidentiality)

要求防止信息的非法泄漏。Security 一词可译为保密,也可译作安全。人们最先意识到出于战争或政治外交的需要,敏感信息不能让敌方获知。应该设法在信息获取、处理、存储、交换的各个环节上对其采取保守机密的措施,以防止信息泄漏给敌人。

2. 信息的完整性(Integrity)

要求防止信息被非法修改和清除。面对现代通信技术与计算机的紧密结合,在以电子化、数字化为基础的信息环境中,人们面对的已不仅是传统的具有纸面签章的书信、文本,越来越多的信息是以计算机处理、储存、传送的。这就产生了这类信息的有效性和完整性问题。

这一问题不能仅靠保密来解决,需要重点发展防止信息被非法修改的技术手段来实施安全保障。

3. 信息的可用性(Avalibility)

要求防止信息重用与拒绝服务。信息意味着财富,在电子资金传送(EFT)系统中直接意味着金钱,这时重用信息就意味着损失了金钱。有效信息的重用可能造成犯罪,必须加以防止。信息系统及其中的信息资源由计算机病毒或其他人为因素造成的拒绝为授权者提供服务将会引起混乱,应该加以防止。反之,发现入侵事件,对非授权者则应该拒绝提供服务。

4. 信息系统的安全可控性(Controlability)

提供信息的合法监控。政府、社会公众出资研究、建设的安全信息系统在用于社会公众时,特别是以商品的形式在市场出售提供公众享用时,社会上的恐怖分子、贩毒集团会借助于市售产品干有损于社会的坏事。这就要求有相应的对策,使管理方有权、有技术手段依法监控信息安全。

由于信息安全内涵的发展,信息系统的模型已从二方系统、三方系统发展到四方系统。

人类最初的信息系统出自于通信的需要。模型由发信者 S(Sender)和收信者 R(Reciever)二方组成。此模型下研究解决的主要问题是信源编码、信道编码、发送设备、接收设备以及信道特性。

由于战争与竞争,存在窃密与反窃密的斗争,信息系统模型中应含第三方——敌人 E(Enemy)。三方模型下,人们还要研究运用密码来保证信息在信道上被窃取后,窃取者不知其意,以保证敏感信息不会泄漏至非授权者。即使面对信息系统及其中的信息,非授权者也看不懂、拿不走、毁不了。

现代信息系统已非政府、军队等专享,社会公众也大量运用其为自己服务。其中可能有贩毒集团、恐怖分子或敌对国,他们借助市售保密设备的保密能力,干起有损于社会的坏事。反过来将政府与管理部门置于敌方 E 的位置之上。这就需要进而考虑第四方——监控管理方 B(Boss)。信息系统的模型因而发展为四方模型(如图 1 所示)。

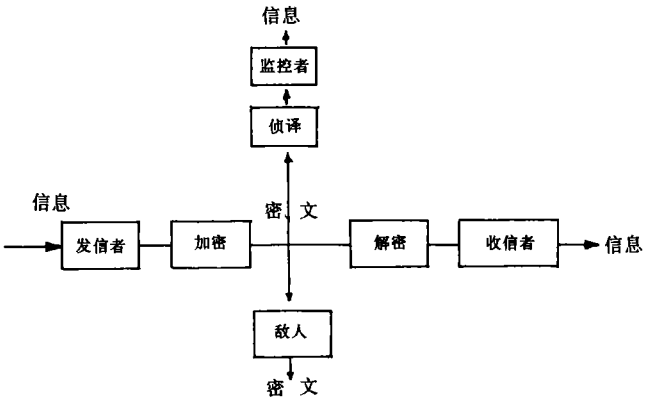

图 1 信息系统的四方模型

为全面保障信息安全,还需要社会关于安全的立法、执法,需要信息系统实体安全的诸种措施,需要人事管理的必要制度,以及环境安全的基础条件。

三、国际上信息安全的研究进展

二次大战以后,密码学研究告别了黑屋时代,成为除政府、军队外,也有学者们积极参与的研究领域。特别是在 70 年代中,美国公布了国家数据加密标准 DES 以及 Deffic—Heleman,提出了公开密钥密码体制的思想。这两大事件促进了密码学的公

开研究，并加速了密码学用于以计算机为基础的现代信息系统、网络通信环境。密码不光是为解决保密才被应用，它还可以用于解决信息的完整性问题、可用性问题，从而成为保障信息安全的最核心的理论基础。

对于信息技术的安全可信性，人们也作了许多深入研究。早在1985年美国国防部(DOD)就公布了可信计算机系统安全评价标准(桔皮书，TCSEC)，其后，DOD所属的国家计算机安全中心(NCSC)又制定并公布了涉及网络安全、数据库安全等方面的一系列安全评价准则的解释与说明，形成了特有的计算机系统安全评价系列丛书——彩虹系列丛书(Rainbow Series)。1992年西欧四国(英、法、德、荷)参照TCSEC制定并公布了信息技术安全评价标准(ITSEC)。它们均把引导信息安全研究、指导公司厂家生产、帮助用户选型、评价系统安全作为综合目标，对信息系统的安全研究与应用起到了非常好的导向作用。1993年美国国家安全局(NSA)和国家标准和技术研究所(NIST)又共同宣布将制定《通用信息技术安全准则》，该准则将吸收TCSEC和ITSEC以及加拿大的CTCPET等的成功经验，并宣称此举的目的是开发可信的信息技术产品，用于保护政府及私人企业的重要信息。这将有助于拓宽这类可信产品的市场，并进一步引导规模经济。

国际标准化组织(ISO)也为有关计算机安全应用作了许多推动工作，组织了许多工作组开展标准化研究指导工作，已出版了有影响的ISO7498—2安全体制结构等。在电子数据交换(EDI)安全、标识卡和信用卡安全、文本和办公室系统安全、操作系统安全、信息技术安全、信息系统安全、银行系统安全等许多方面着手制定了标准草案。

国际上在信息安全研究方面取得的许多成果，积累的许多经验，生产的许多用于保证信息安全的产品，可以供我们借鉴和应用。

四、“三金工程”中实施信息安全保护的思考

就金桥工程而论，虽然有许多行业、部门的网络可能是专用网，但是将许多子网汇合起来的网络环境可能是公用信息网，起码是一个由许多行业部门共享的信息网。在网上，从功能来看存在着通信子网与资源子网。

就解决网络信息安全问题看，应该在通信子网与资源子网间构作起安全子网(如图2)。

安全子网应该考虑具备以下重要安全功能：网络用户登录、访问控制、授权管理、敏感信息的通信加密、通信信息的完整性保障、密钥管理、安全事件的审计跟踪和安全监控。

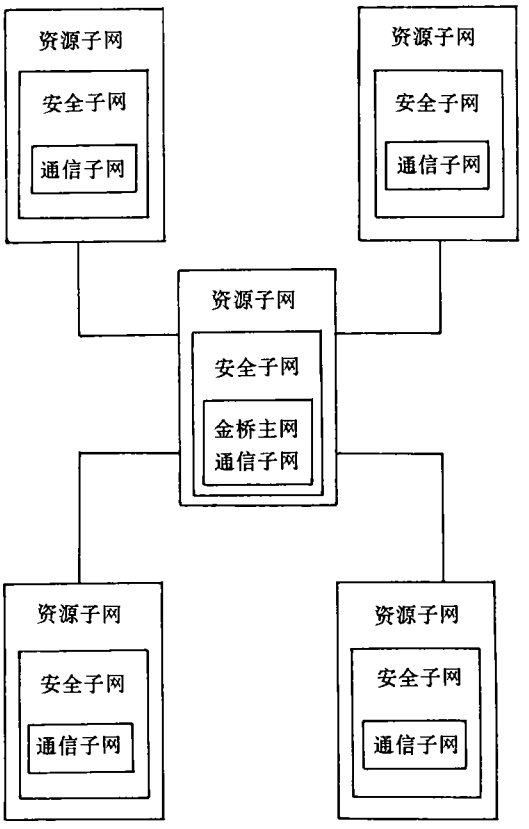

图2 安全网构作示意图

就资源子网论，也应重视信息安全保护。资源可能是大型主机(HOST)，可能是用户工作站(Workstation)、个人微型计算机(PC)。HOST系统一般是专用操作系统，具有一些初步的安全功能。最脆弱的环节是运行DOS操作系统的PC。由于DOS的开放性，具备一般操作知识与经验的人很容易进入系统，干自己想干的事，更不要说那些存心侵入的具备较深专门知识的攻击者了。因此，根据TCSEC和ITSEC的思想，首先要在可信计算基(TCB)上着手，而操作系统安全性是其核心和基础，进而要考虑集中提供信息资源存储与查询功能的数据库的安全性。

TCSEC中提出了解决安全需求的许多安全策略，可以为我们所用的系统主要有：

1. 自主访问控制(Discrctionary Access Control) 根据需要(Need—to—Know)安排主体可否访问客体。常以Self、group、pubfic代码标出主体对客体的读、写、删、创建的可否。可用于简单的访问控制安全性授权管理。

2. 强制访问控制(Mandatory Access Control) 对于多级安全的系统，要把主体与客体分割为不同的保密层次，一个主体可读一个客体，仅当主体的安全级高于或等于客体的安全级别；一个主体可

写一个客体，仅当主体的安全级别低于或等于客体的安全级别。为实现以上原则还需要身份识别和验证来配合。

3. 标识(Labels) 对于主体与客体(用户、进程、文件、段、装置等)作上敏感度的标识，以便于实行强制访问控制时，作为安全级别判断的依据。为输入一个无标识的数据需要从授权用户接收一个数据的安全级，并将此活动进行审计。

4. 身份识别与验证(Identification and Authentication) 身份识别是在允许用户进入信息系统开始任何活动时判断是谁。验证是使用保护机制进一步断定其身份的真伪，真则可依其授权进行访问操作，是假则必须拒绝访问，每个允许进入系统的用户必须有唯一的身份以便于记帐。TCB 适应提供对相应身份识别的审计能力。

5. 审计(Audit) TCB 可以创建、维护和保护、修改未授权的访问或消毁保护对一个客体的访问的一个审计跟踪。审计数据被TCB 保护，这样，对审计数据的读、访问将限制在被授权者。TCB 可以记录以下类型事件：身份识别与验证方法的使用，导引客体进入用户的地址空间(打开文件，程序初始化)，依靠计算机操作系统检测客体的活动，监控系统安全官员及其他安全事件。对每一个记录的事件，审计记录将识别：事件的日期与时间、用户、事件类型、事件成功或失败。对于身份识别与验证事件的原始需求发起者(如终端 ID)将记于审计记录。对于引导一个客体进入用户地址空间或删除一个客体，审计记录应包含客体名。自动数据处理(ADP)系统的监控者可以选择对一个或更多的独立身份用户进行审计活动。

此外系统还要从系统体系结构、系统完整性、隐通道分析、可信设施管理、可信恢复等方面提供安全操作保障，并用安全性测试来提供系统生命周期中的安全保障，以及在系统设计与修改时提供安全性说明。

综上所述，包括操作系统安全、数据库安全和网络安全在内的信息系统的安全性是信息安全的技术保障。它可以用实施由各种安全策略组成的安全机制构成的安全服务功能来实现。密码理论与技术是保证信息安全的核心基础。由于实施安全服务会带来系统的时空资源开销，并带来相应的资金花费，因而根据实际需要构作可满足安全应用的相应安全级别的系统是平衡安全需求与开销、效率的必要方法。TCSEC 及 ITSEC 均把安全级别界定为六或七级(前者由 D、C1、C2、B1、B2、B3、A1 组成，后者由 E1～E6 组成)，不同级别采用不同的安全策略。

就金关而论，除了要依托于上述系统安全的支撑，我们认为应着重强调其电子数字数据的有效性并在必要环节利用密码解决信息加密。

我们将四方模型进一步展开为适应有效性公证与仲裁的系统模型(见图 3)。

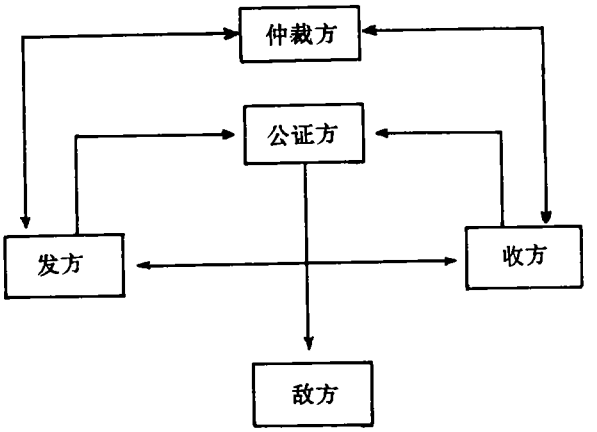

图 3 有效性系统模型

有效性涉及到真实性、不可伪造、不可改变和不可重用。在合同、契约及电子支付应用中成为要害问题。在电子化、数字化的运作机制下更是关键。要有立法执法的保证，但这远远不够，还必须依靠高科技手段来加以保障，以防止社会犯罪造成的损失。最佳的解决有效性的基础是利用公开密钥密码体制来进行数字签名，并利用 Hash 函数生成信息验证码(MAC)来保证完整性。MAC 使得数据即使有 1 比特被改动也能查觉，由于签名是发送者唯一拥有的私钥的派生物，别人不能仿冒，责任自然分明。防止重用则要利用时间印记等方法来标明时效。

模型中各方的工作及责任如下：收发方均应向公证方提交公证依据(即各自的私钥)，当发方以其私钥进行数字签名后，收方可以发方的公钥进行解密。一般情况下由于发方私钥只有他自己拥有，别人无法作出同样的签名，收方就可认可。反过来把收到的回执以收方私钥签名送回。依同理发送收到后也应认可。若出现纠纷有其中一方企图抵赖，仲裁方可从公证方取证，以某私钥确系某方独有来裁定其抵赖的责任。私钥代替了纸面的签名、盖章。收发方及公证方必须对其严格保密。

就金卡而论其安全性的关键是个人识别号(PIN)的保密与安全，原则上说磁卡的安全性没有 IC 卡高，则 IC 卡中带有处理器(CPU)的卡的安全性又高于仅有存储能力的卡。

为了保证银行金融卡的安全性，对其关键信息 PIN 的安全管理要遵循如下基本原则：(1)对被用于 PIN 管理与控制功能的所有硬件与软件均不能被欺骗性地使用或未经记载的访问、检测和失去功能。(2)PIN 被选择后，若要存储必须进行加密，并遵守一定的物理安全要求。(3)对于不同的帐户，同样的 PIN 值在给定的加密密钥加密时不能产生相同的密

(下转第 11 页)

不在运用分子生物学的概念和技术，并且无一不在逐步走向结构生物学，而分子生物学和结构生物学诞生本身又是得益于物理学的成就。再举一个例子，看看国际上是如何看待生物物理学和生物化学的关系的。在1993年布达佩斯国际生物物理学大会的五个大会报告中四个是关于蛋白质结构研究的，唯一的从表面上看似乎是非蛋白质的大会报告，是日本大阪SANGYO大学信息系统工程系的义泽(Yoshizawa)教授作的"颜色视觉分子基础"，显然这是神经生物学的内容，但它的基本实验是测定鸡的各种视锥色素蛋白和壁虎的两种视觉色素蛋白的氨基酸序列，结果发现后者是视锥色素蛋白。他在此基础上，构建了视觉色素蛋白的系统发育进化树，阐明了视锥色素蛋白要比视杆色素蛋白(rhodopsin)进化更早，说明颜色视觉和光视觉要比微光视觉更早。他还根据氨基酸序列计算的电荷，推测进化过程中由于酸性氨基酸取代了碱性氨基酸而发生视锥色素蛋白向视杆色素蛋白的转变。比较鸡的视锥色素蛋白和视杆色素蛋白的"漂白"过程发现后者的中间物Ⅱ的寿命较长，从而解释了为什么视杆色素蛋白对光有较高的敏感性。这个由信息系统工程系的科学家做的有关视觉机理的研究，是建立在"蛋白质分子结构基础"上的，其工作内容，蛋白质的序列分析，似乎完全"应该"归类于生物化学范畴，却恰恰被国际生物物理大会认为是近三年来生物物理学领域内最优秀的成果之一而选作大会报告。

今天，生命科学家的任务是要运用人类所有的对自然，特别是对生命的知识和认识，运用人类已经掌握的全部技术来研究生命，而不能只固守在自己已经习惯的一小块领地上，只遵循自己一贯的概念，只用自己熟悉的方法进行工作，那是不能进步的，也不能为科学发展做出贡献。我国生物学家也只有适应国际潮流，与其他姐妹学科相互渗透携手前进才能向新的高度进军。

建立结构生物学研究中心刻不容缓

在不久前举行的以结构生物学为主题的中国科学院香山会议上，到会专家一致呼吁刻不容缓地在中国建立结构生物学研究中心。

1953年分子生物学时代开始，60年代突飞猛进，可是我国不但没有立即作出反应，十年动乱期间反而对这一新兴学科进行了违反科学的批判。1976年"文化大革命"结束后，经过一些科学家的呼吁，才逐渐对分子生物学的发展给以一定的重视，但直到1987年才在上海生物化学所建立分子生物学国家重点实验室。国际上从1953到1987的30余年间分子生物学的飞速发展，不仅造成了我国在这一重要基础研究领域与国际先进水平的巨大差距，也是我国当前生物高新技术产业举步维艰的根本原因。

与1953年我国的分子生物学水平相比，我国当前在结构生物学上应该说已有相当基础。生物大分子国家重点实验室在蛋白质晶体结构分析、溶液构像变化与生物活性关系以及膜蛋白等方面已经做出了一批较高水平的成果，曾多次被重要国际会议邀请做大会报告或特邀报告，并被邀请在国际核心刊物上撰写有关领域的综述性论文，因此在国际上享有一定的声誉。另外，在电子显微镜、隧道电子显微镜、各种光谱技术等方面我国也有相当好的实验室。

现在国际上结构生物学的新时代开始还不太久，应该认真吸取我国在1953年对待分子生物学的惨痛教训，从速以生物大分子国家重点实验室为核心，组织国内各单位高水平的研究课题，给以足够强度的投资，建立跨单位的结构生物学研究中心。这样我们才可能保持我国在某些领域内的国际先进地位，并且经过努力，建成在国际上举足轻重的研究中心。由于结构生物学对生命科学的全面影响，它也必将推动我国生命科学的全面发展。可以预见，在今后一个不太长的时间内，结构生物学必然会出现像当年分子生物学一样的辉煌。希望那个时候，全人类共享的成果中也有中国科学家贡献的光和热。

（责任编辑　蔡德诚）

（上接第32页）

文。(4)一个被加密的PIN的安全性不仅依赖于加密设计或算法安全，而主要靠密钥的保密。(5)PIN的明文绝不可存在于获取装置之中，除非装置具有物理安全。(6)只有客户个人才能被卡的发行人授权选择PIN。PIN的颁发或任何与帐户识别信息相关的登记处理，均能保证使个人操作在安全强制过程中进行。(7)存储的加了密的PIN将被替换保护。(8)PIN的泄露只能发生在其生命周期的结束。(9)PIN校验的责任取决于发行者可否通过校验功能代表其他人设定。(10)对PIN的存储和加密必须使用不同的加密密钥。(11)在PIN和PIN的保密无效写入时应告知客户。

（责任编辑　王宏章）