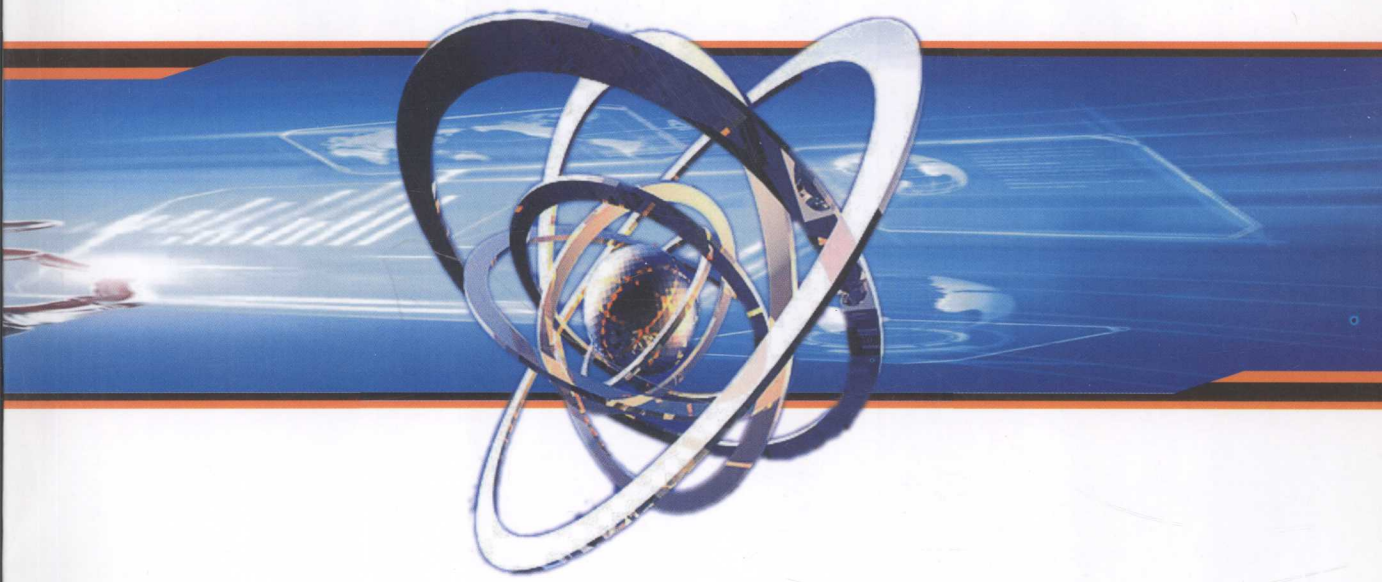
高等学校规划教材·计算机科学技术

PROGRAMMING TEXTBOOKS FOR HIGHER EDUCATION



信息安全政策与法规

王 成 陶林伟 苟燕妮 编

西北工业大学出版社

高等学校规划教材·计算机科学技术

信息安全政策与法规

王　成　陶林伟　苟燕妮　编

西北工业大学出版社

【内容简介】 本书以信息安全通常采取的安全措施(对策)为主线,系统地介绍了信息安全知识和技术,重点介绍了信息系统的安全运行和网络信息的安全保护,内容包括信息安全概述、网络安全法律法规、黑客和病毒、现代密码学、常规加密技术与应用、公钥加密技术、防火墙、电子邮件安全和IP安全以及身份认证等。

本书内容安排合理,逻辑性强,语言通俗易懂,书中实例的应用性和可操作性较强,便于教学和自学。

本书可作为高等院校计算机类专业本科生的教材,也可作为网络管理人员、网络工程技术人员、信息安全管理人员以及对网络安全感兴趣的一般读者的参考书。

图书在版编目(CIP)数据

信息安全政策与法规/王成,陶林伟,苟燕妮编. —西安:西北工业大学出版社,2014.1
ISBN 978-7-5612-3903-2

Ⅰ.①信… Ⅱ.①王… ②陶… ③苟… Ⅲ.①信息安全—方针政策—中国 ②信息安全—法规—中国 Ⅳ.①TP309②D922.14

中国版本图书馆CIP数据核字(2014)第012929号

出版发行:西北工业大学出版社
通信地址:西安市友谊西路127号 邮编:710072
电 话:(029)88493844 88491757
网 址:www.nwpup.com
印 刷 者:陕西宝石兰印务有限责任公司
开 本:787 mm×1 092 mm 1/16
印 张:8.75
字 数:207千字
版 次:2014年6月第1版 2014年6月第1次印刷
定 价:25.00元

前　言

信息安全是一个不断发展和丰富的概念，它经历了从保密通信、计算机安全、信息安全到信息保障的演变。信息安全的需求也从保密性扩展到完整性、可用性、不可否认性和可控性。人们在不断探索和发现各种技术来满足信息安全需求的同时，逐渐认识到信息安全是一个综合的多层面问题。一个完整的国家信息安全保障体系应该包括信息安全法制体系，组织管理体系，基础设施、技术保障体系，经费保障体系和安全意识教育人才培养体系。

要保障信息安全，“三分靠技术，七分靠管理”，足见管理是信息安全保障的关键。信息安全管理的原则体现在政府制定的政策法规和机构部门制定的规范制度上。同时，信息安全技术蓬勃发展，形成了一个新的产业，规模化的信息安全产业发展需要技术标准来规范信息系统的建设和使用，生产出满足社会广泛需求的安全产品。

本书从信息安全政策与法规开始，引入信息安全的概念和应用，在内容选取上，既注意理论的系统性，又兼顾材料的多样性，突出了理论与实践的结合，并且在传统信息安全政策与法规的基础上加入了案例分析，彰显了特色。

本书分为 9 章，内容安排如下：

第 1 章主要阐述了信息安全的有关概念，包括信息安全的定义、特征、内容、体系结构等。

第 2 章介绍了网络安全相关的法律法规，包括案例分析、我国网络安全立法体系框架、计算机犯罪的防范和打击、网络安全管理要求、安全服务及产品的管理要求、信息系统安全等级保护的基本技术要求、中华人民共和国电子签名法等。

第 3 章介绍了黑客和病毒，内容包括以往计算机病毒的特点分析以及今后病毒的发展趋势、黑客的概念及常用的入侵方法和采取的应对安全措施。

第 4 章介绍了现代密码学，主要介绍密码学基本概念，密码体制的分类，密码攻击(分析)，密码学的起源、发展及实例，密码学的现状和发展趋势。

第 5 章介绍了常规加密技术与应用，这一章是本书的重点章节，主要内容有现代密码学概论、常规加密技术理论与算法实现、加密技术的应用等。

第 6 章介绍了公钥加密技术，主要介绍了非对称加密算法原理，RSA 算法的原理及算法实现、Diffie - Hellman 密钥交换算法及其他非对称密码算法的原理。

第 7 章介绍了防火墙，包括防火墙的概念、功能和类型，防火墙技术，防火墙的体系结构，防火墙的选择，防火墙的发展趋势及应用。

第 8 章介绍了电子邮件安全和 IP 安全，包括电子邮件安全的概念、加密方法及实现手段，IP 安全的结构、关键参数、密钥交换等。

第 9 章介绍了身份认证技术，包括身份认证技术概述、基于口令的身份认证、Kerberos 身份认证协议、基于 X509 的身份认证以及基于生物特征的身份认证等。

在本书编写过程中，参阅了大量国内外相关的资料和文献，在此对这些参考资料的作者深表谢意！

由于水平有限，书中难免有不妥之处，敬请读者批评指正。

编　者

2014 年 5 月

目　录

第1章　信息安全概述

信息是人类的宝贵资源，是否能大量而有效地利用信息是衡量社会发展水平的重要标志之一，也是影响国家综合实力的重要因素。对信息的开发、控制和利用是信息处理的主要目标，但如何有效地保护信息的安全也是很重要的研究课题，是国家现在与未来安全保障的迫切需求。

信息安全指的是保护计算机信息系统中的资源（包括计算机硬件、计算机软件、存储介质、网络设备和数据等）免受毁坏、替换、盗窃或丢失等。信息系统的安全主要包括计算机系统的安全和网络方面的安全。随着网络的不断发展，全球信息化已成为人类发展的趋势。由于网络具有开放性和互联性等特征，使得网络易受计算机病毒、黑客、恶意软件和其他不轨行为的攻击，因此信息系统的安全也就成为了一项很重要的工作。

1.1　信息安全定义

信息是一种资产，同其他重要的商业资产一样，它对其所有者而言具有一定的价值。信息可以以多种形式存在，它能被打印或者写在纸上，能够数字化存储，也可以由邮局或者用电子方式发送，还可以在电影中展示或者在交谈中提到。无论以何种形式存在，或者以何种方式共享或存储，信息都应当得到恰当的保护。

国际标准化组织和国际电工委员会在“ISO/IEC17799：2005”协议中对信息安全的定义是这样描述的：“保持信息的保密性、完整性、可用性；另外，也可能包含其他的特性，例如真实性、可核查性、抗抵赖和可靠性等。”

对信息安全的描述大致可以分成两类：第一类是指具体的信息技术系统的安全，而另一类则是指某一特定的信息体系（如银行信息系统、证券行情与交易系统等）的安全。但也有人认为这两种定义都不全面，而应把信息安全定义为：一个国家的社会信息化状态与信息技术体系不受外来的威胁与侵害。作为信息的安全首先是一个国家宏观的社会信息化状态是否处于自主控制之下、是否稳定的问题，其次才是信息技术安全的问题。

因此，信息安全的作用是保护信息不受到大范围的威胁和干扰，能保证信息流的顺畅，减少信息的损失。

1.2　信息安全特征

无论入侵者使用何种方法和手段，他们的最终目的都是要破坏信息的安全属性。信息安全在技术层次上的含义就是要杜绝入侵者对信息安全属性的攻击，使信息的所有者能放心地使用信息。国际标准化组织将信息安全归纳为保密性、完整性、可用性和可控性四个特征。

保密性是指保证信息只让合法用户访问，信息不泄露给非授权的个人和实体。信息的保密性可以具有不同的保密程度或层次，所有人员都可以访问的信息为公开信息，需要限制访问的信息一般为敏感信息，敏感信息又可以根据信息的重要性及保密要求分为不同的密级，例如国家根据秘密泄露对国家经济、安全利益产生的影响，将国家秘密分为“秘密”“机密”和“绝密”三个等级，可根据信息安全要求的实际，在符合《国家保密法》的前提下将信息划分为不同的密级。对于具体信息的保密性还有时效性要求等(如保密期限到期了即可进行解密等)。

完整性是指保障信息及其处理方法的准确性、完全性。它一方面是指信息在利用、传输、存储等过程中不被篡改、丢失、缺损等，另一方面是指信息处理的方法的正确性。不正当的操作，有可能造成重要信息的丢失。信息完整性是信息安全的基本要求，破坏信息的完整性是影响信息安全的常用手段。例如，破坏商用信息的完整性可能就意味着整个交易的失败。

可用性是指有权使用信息的人在需要的时候可以立即获取。例如，有线电视线路被中断就是对信息可用性的破坏。

可控性是指对信息的传播及内容具有控制能力。实现信息安全需要一套合适的控制机制，如策略、惯例、程序、组织结构或软件功能，这些都是用来保证信息的安全目标能够最终实现的机制。例如，美国制定和倡导的“密钥托管”“密钥恢复”措施就是实现信息安全可控性的有效方法。

不同类型的信息在保密性、完整性、可用性及可控性等方面的侧重点会有所不同，如专利技术、军事情报、市场营销计划的保密性尤其重要，而对于工业自动控制系统，控制信息的完整性相对其保密性则重要得多。

确保信息的完整性、保密性、可用性和可控性是信息安全的最终目标。

1.3 信息安全内容

信息安全的内容包括了实体安全与运行安全两方面的含义。实体安全是保护设备、设施以及其他硬件设施免遭地震、水灾、火灾、有害气体和其他环境事故以及人为因素破坏的措施和过程。运行安全是指为保障系统功能的安全实现，提供一套安全措施来保护信息处理过程的安全。信息安全的内容可以分为计算机系统安全、数据库安全、网络安全、病毒防护安全、访问控制安全、加密安全六个方面。

计算机系统安全是指计算机系统的硬件和软件资源能够得到有效的控制，保证其资源能够正常使用，避免各种运行错误与硬件损坏，为进一步的系统构建工作提供一个可靠安全的平台。

数据库安全是指对数据库系统所管理的数据和资源提供有效的安全保护。一般采用多种安全机制与操作系统相结合，实现数据库的安全保护。

网络安全是指对访问网络资源或使用网络服务的安全保护，为网络的使用提供一套安全管理机制。例如，跟踪并记录网络的使用，监测系统状态的变化，对各种网络安全事故进行定位，提供某种程度的对紧急事件或安全事故的故障排除能力。

病毒防护安全是指对计算机病毒的防护能力，包括单机系统和网络系统资源的防护。这种安全主要依赖病毒防护产品来保证，病毒防护产品通过建立系统保护机制，达到预防、检测和消除病毒的目的。

访问控制安全是指保证系统的外部用户或内部用户对系统资源的访问以及对敏感信息的访问方式符合事先制定的安全策略，主要包括出入控制和存取控制。出入控制主要是阻止非授权用户进入系统；存取控制主要是对授权用户进行安全性检查，以实现存取权限的控制。

加密安全是为了保证数据的保密性和完整性，通过特定算法完成明文与密文的转换。

例如，数字签名是为了确保数据不被篡改；虚拟专用网是为了实现数据在传输过程中的保密性和完整性而在双方之间建立的唯一的安全通道。

1.4　OSI信息安全体系结构

为了适应网络技术的发展，国际标准化组织的计算机专业委员会根据开放系统互连OSI参考模型制定了一个网络安全体系结构《信息处理系统开放系统互连基本参考模型第二部分——安全体系结构》，即ISO 7498—2，它主要解决网络信息系统中的安全与保密问题，我国将其作为GB/T 9387—2标准，并予以执行。该模型结构中包括五类安全服务以及提供这些服务所需要的八类安全机制。

安全服务是由参与通信的开放系统的某一层所提供的服务，是针对网络信息系统安全的基本要求而提出的，旨在加强系统的安全性以及对抗安全攻击。ISO 7498—2标准中确定了五大类安全服务，即鉴别、访问控制、数据保密性、数据完整性和禁止否认。

鉴别服务用于保证双方通信的真实性，证实通信数据的来源和去向是我方或他方所要求的和认同的，包括对等实体鉴别和数据源鉴别。

访问控制服务用于防止未经授权的用户非法使用系统中的资源，保证系统的可控性。访问控制不仅可以提供给单个用户，也可以提供给用户组。

数据保密性服务的目的是保护网络中各系统之间交换的数据，防止因数据被截获而造成泄密。

数据完整性服务用于防止非法用户的主动攻击（如对正在交换的数据进行修改、插入，使数据延时以及丢失数据等），以保证数据接收方收到的信息与发送方发送的信息完全一致。它包括可恢复的连接完整性、无恢复的连接完整性、选择字段的连接完整性、无连接完整性、选择字段的无连接完整性。

禁止否认服务用来防止发送数据方发送数据后否认自己发送过的数据，或接收方接收数据后否认自己收到过数据。它包括不得否认发送和不得否认接收。

安全机制可以分为两类，一类与安全服务有关，是实现安全服务的技术手段；另一类与管理功能有关，用于加强对安全系统的管理。ISO 7498—2提供了8大类安全机制，分别是加密机制、数据签名机制、访问控制机制、数据完整性机制、认证交换机制、防业务填充机制、路由控制机制和公证机制。

第2章 网络安全法律法规

2.1 典型案例

案例1:网络盗窃

丽水的女网民潜某在淘宝网上盗窃文成县金某的游戏充值卡11万余元,贱卖后非法获利6万余元供自己挥霍。这名自以为神不知鬼不觉的女黑客很快就落入法网,被文成县人民法院一审判刑10年,并处罚金2万元。

2008年2月20日晚9时许,潜某在丽水市莲都区灯塔小区其家中,通过密码找回的功能,破解了金某在淘宝网上的用户名"llm78"的密码,并修改了该用户名的密码。次日凌晨,潜某在丽水市阳光地带网吧及其家中,用修改后的密码登录"llm78"的用户名,窃取了金某所有的1 457张"征途"游戏充值卡和70张盛大游戏充值卡,并在网上以5至6折的价格出售,非法获利6万余元人民币。

第二天早上,金某发现自己的用户名llm78已不能登录,经与淘宝的管理员联系后终于登录上去,但发现里面的游戏卡都已被使用。淘宝管理员为他提供了一些账号登录的信息,金某随后到文成县公安局报案。网监大队的民警通过淘宝网交易的上网IP地址,发现交易在丽水进行,迅速锁定了这名女黑客,并前往丽水将潜某抓捕归案。

经文成县涉案物品价格认证中心鉴定,金某被盗游戏充值卡的价值为人民币11.7万元。案发后,潜某家属赔偿了经济损失计人民币6万元。

文成县人民检察院以盗窃罪对潜某提起了公诉,要求追究其刑事责任。法院经审理认为,潜某以非法占有为目的,通过破解密码的方式,盗取他人能实现财产价值的财物,数额特别巨大,其行为已构成盗窃罪。鉴于家属对经济损失作了部分赔偿,酌情从轻处罚。判处潜某有期徒刑10年,并处罚金人民币2万元,同时责令潜某退赔违法所得给金某。

案例2:网络诈骗

4名少年痴迷网络游戏,在互联网上以出售网络游戏装备为名,数十次诈骗他人钱财。近日,安徽马鞍山市花山区人民法院审结了这起网络诈骗案,依法对4名被告人判刑。

马鞍山市花山区人民法院审理查明,马某、周某、张某和陈某四人出生于上世纪80年代,都痴迷网络游戏。因玩游戏花钱,四人商量利用网络骗钱。随后,他们办理了假身份证,利用伪造证件在银行开设账户,购买手机卡。同时,四人还在网上申请了网站,挂上了各种网络装备、金币的信息,以骗取被害人信任。2008年4月,被告人在一款名为《诛仙》的网络游戏中,以255元低价出售网络装备。受害人与被告人达成一致意见后,向被告人银行账户汇入255

元。但被告人以银行账户无法激活为借口，要求对方必须再汇款激活账户，激活后再将钱款退回，先后 9 次骗得受害人人民币 15 800 多元。2008 年 7 月，被告人又在一款名为《魔兽世界》的网络游戏中，以低价代刷游戏装备为由，骗取受害人 1 100 元，又以激活银行账户为由骗取对方 16 400 多元。四人先后实施诈骗 20 多次，诈骗总金额达 6 万多元。2008 年 7 月 18 日，4 名被告人被抓获。经公安机关查明，马某曾有网络诈骗前科，被法院判处拘役 4 个月，宣告缓刑 1 年。

法院经审理认为，4 名被告人以非法占有为目的，采取虚构事实、隐瞒真相的方法骗取他人财物，构成诈骗罪。其中，马某、周某骗取他人现金人民币 35 000 多元，数额巨大，张某和陈某诈骗金额 26 000 多元，数额较大。法院遂依法宣判。马某被判处有期徒刑 3 年 6 个月，罚金 3 万元，周某被判处有期徒刑 3 年，宣告缓刑 3 年，罚金 2 万元，其他两名被告人被判处缓刑。

案例 3：网络虚拟财产的保护

2003 年 2 月 17 日，网络游戏《红月》的玩家李某发现自己游戏中所有装备被盗。他感到自己的权利遭到了侵犯，就将运营商北极冰公司起诉至北京市朝阳区法院，要求对方赔偿丢失的装备，公开赔礼道歉。北京市朝阳区法院受理了此案并于当年 12 月 18 日作出一审判决，认定被告侵犯虚拟财物的事实成立，但因虚拟财产的价值在现实生活中没有统一标准，故判定被告在判决生效 7 日内恢复原告丢失的武器装备。

网络游戏自 1999 年正式登陆中国，现在已经形成一个庞大、高速增长的新兴市场，但是因“网财”而衍生的纠纷更是层出不穷，“网财”的保护已经是个迫在眉睫的问题。为了网络游戏业的健康发展，必须加强对“网财”的立法保护，事实上，立法的滞后，在某种意义上已经制约了我国游戏产业的快速发展，可以想象，如果我们能够尽快地完善立法，加强对“网财”的保护，必将大大促进我国游戏产业的更快发展，使其成为我国经济的新的增长点。

现在保护“网财”我们所能依据的只是《宪法》和《民法通则》以及 2000 年底全国人民大会常务委员会制定的《关于维护互联网安全的决定》（以下简称《决定》）的笼统规定，即 2004 年修正后的中华人民共和国宪法第十三条有关规定：“公民的合法的私有财产不受侵犯。国家依照法律规定保护公民的私有财产权和继承权。”这一合法私有财产的概括规定为民法财产的解释提供了极大的空间；《民法通则》第 75 条规定：“公民的个人财产，包括公民的合法收入、房屋、储蓄、生活用品、文物、图书资料、林木、牲畜和法律允许公民所有的生产资料以及其他合法财产。”然而对于“其他合法财产”，我国法律并无明确的解释，也给我们对其解释提供了空间；2000 年的《决定》第四条规定利用互联网犯罪，追究刑事责任；侵犯他人合法权益，依法承担民事责任。这个《决定》对“网财”的保护依然没有明确，但是也没有否定对“网财”的保护，这同样也给司法解释提供了空间。至于《消费者权益保护法》，虽然规定了消费者的多达 9 项权利，但是游戏者对其“网财”的权利并没有包括在内。当然，游戏者和游戏商的关系也是一种消费关系，但是依靠该法并不能保护游戏者的权益，更何况，“网财”被侵犯不仅涉及游戏商和游戏者，还常常涉及第三方，也因而往往超出了该法的调整范围。

面对当前立法现状，只有加强立法，尽快针对急需问题颁布相关法律和司法解释予以规范，特别是在指导打击网络犯罪的刑事方面。建议先尽快颁布司法解释，待条件成熟时再立法，因为毕竟立法是一项系统工程，需要经过建议、计划、草案等诸多环节，旷日持久，因而无法

解决现在面临的问题。司法解释并非创立新法，可以较快制定，程序也较为简单。前文已述，我国现行的法律规定也为先从司法解释的角度对“网财”进行保护提供了可能。

在最高人民法院和最高人民检察院进行司法解释的时候，首先应当明确“网财”的属性。司法解释应当明确规定该财产属于《民法通则》第75条合法财产的一种，在某种意义上可以认为是公民合法收入的一种，《刑法》第92条规定的所谓公民私有财产是包含该财产权的，从而为民法和刑法对“网财”的保护提供了客观的科学依据。同时，由于现代社会经济和科学技术的发展，狭义概念的物已经不符合实际生活的需要，这样解释也在理论上廓清了其可以作为物权的客体，消除了理论上对“网财”法律属性的争论，也符合现状。其次应当明确这种无形财产价值的计算方法，必要时，可以成立或者指定专门的机构予以评估。若其价值无法认定，将无法适用《民法通则》特别是《刑法》等法律条文予以保护。但相关案件不断发生，为指导司法实践、统一司法者的认识，必须尽快解决虚拟物品的价值认定问题。在具体解释时，最迫切的是刑法的解释应当尽快出台，因为在涉及虚拟网络的民事审判中还可依靠法官自由裁量，而在涉及虚拟网络的刑事案件则因法无明文规定无法处理，事实上造成对罪犯的放纵，在很多地方有的网民发现自己的“网财”被盗去派出所报案，而派出所则因“网财”的保护法律没有规定而且价值不能确定，则无法处理将报案人拒之门外，不能不让法律工作者扼腕叹息。此外这个法律上的空白也助长和刺激了对“网财”的肆意侵犯，诸如网上的盗窃、诈骗等的犯罪不断发生。对于“网财”的民法的保护，鉴于我国正在制定民法典，如果条件成熟可以考虑先于刑法在民法典中做出适当的规定。

总之，“网财”的保护是私有财产入宪以后一个很现实、很重要的问题，因为这不仅关系到网络游戏玩家和游戏商的利益，还关系到网络游戏的长远发展，关系到我国国民经济的长远发展，我们只有顺应新技术的发展要求，对传统制度做出因时制宜的修改，赋予其新的生命力，在社会各方特别是立法机关的共同努力下才能真正促进对“网财”的保护。

案例4：网络赌博案

从国外赌博网站取得网络赌博代理权，形成以股东形式为结构的坐庄赌博犯罪团伙。公诉机关指控，该团伙账号下管理的投注金额高达1.6亿多元。16日上午9点，涉案的8名被告人在天津市和平区人民法院受审。其中被告人刘某、魏某、宫某系女性。

公诉机关指控，2011年，被告人高某从菲律宾“太阳城”赌博网站上级代理处取得两个管理账号的网络赌博代理权，代理网络百家乐赌博活动。后发展被告人徐某、任某及王某、李某（另案处理）形成以股东形式为结构的坐庄赌博犯罪团伙，并于同年6月制作生成一坐庄管理账号。为达到非法营利目的，该团伙又积极发展被告人张某等人为下级代理，并利用坐庄管理账号为被告人张某制作生成下级管理账号。

至2011年7月案发，被告人高某、任某坐庄管理账号下的投注金额为1.6亿多元。被告人张某管理账号下的投注金额为479万多元。2011年7月13日，被告人高某利用其管理的账号，为被告人刘某制作生成下级管理账号，发展被告人刘某为下级代理。被告人刘某又利用管理账号制作生成两个会员账号，发展被告人魏某为下线参与网络百家乐赌博投注活动。魏某以营利为目的，在天津市河北区王串场某小区，组织杜某、倪某等多人使用两个会员账号，登录菲律宾“太阳城”赌博网站，进行网络百家乐赌博投注活动，至2011年7月15日案发，魏某两个会员账号下的投注金额为48万多元。

2011 年 4 月至 7 月间，被告人宫某以营利为目的，在天津市和平区南京路某地和河北区王串场某小区，组织存某、许某等人，通过电话或传真上报给上家的方式，进行网络六合彩特码赌博投注活动，至 2011 年 7 月 15 日案发，宫某代为投注金额为 45 万多元。

2011 年 5 月至 7 月间，被告人周某以营利为目的，在天津市河北区某小区，组织李某、邱某等人使用其从上家获得的账号，登录网上六合彩赌博网站，进行网络六合彩特码赌博投注活动，至 2011 年 7 月 15 日案发，周某账号下的投注金额为 8 万多元。经群众举报，公安机关于 2011 年 7 月 15 日将任某、徐某等人抓获，7 月 29 日将高某抓获。

法庭上，本案公诉人认为，应当以开设赌场罪追究被告人高某、任某等人刑事责任，以赌博罪追究被告人魏某、宫某等人刑事责任。

面对公诉机关指控，8 名被告人对其所犯罪行均供认不讳。高某辩护人、天津市国浩（天津）律师事务所王建人律师辩称，证据显示，王某、徐某、任某等人先是一起商量在网络上坐庄赌博，然后决定由高某去找个账号，并不是高某先取得账号再发展其他 4 个股东坐庄赌博犯罪。高某、王某等被告是下级代理主动申请成为其一级代理。王律师表示，被告人从有账号实施网络赌博至案发，仅 26 天时间，时间短，发展的赌博级别少，虽然投注额大，但实际投入赌资很少，故不应认定为“开设赌场情节严重”。

案例 5：破坏计算机信息系统案

刑法修正案（七）公布实施前对于制作、传播木马程序，影响计算机系统正常运行，后果严重的，以破坏计算机信息系统罪定罪处罚。修正案公布后，增加了非法获取计算机信息系统罪和提供侵入计算机信息系统程序、工具罪等两款规定，对制作、传播木马程序行为产生不同法律认定。因此，对于该刑法修正案公布前实施而在公布后审理的通过制作、提供专门用于侵入计算机信息系统的木马程序以及利用传播木马程序获取他人存储、处理或者传输的数据，情节严重的行为，应当根据刑法从旧兼从轻的溯及力原则，分别以提供侵入计算机信息系统程序罪和非法获取计算机信息系统数据罪论处。

2007 年 6 月，被告人吕某、曾某开始开发用于盗取网络游戏账号、密码的木马程序，到 2008 年初该程序开发成功，并由曾某出面寻找合作伙伴帮助销售。2008 年 2 月起，被告人严某接受曾某的委托，将该系列木马程序命名为“温柔”木马并总代理销售，同时按照游戏种类分包给不同的一级代理商张某、张某某等人，按照包用时间收费，谋取非法利益。2008 年 6 月，被告人陈某参与经营，与严某共同代理销售“温柔”系列木马。吕某等人开发并销售的“温柔”系列木马种类达 30 余款，盗窃游戏账号、密码数百万组。被告人丁某、许某、林某在明知严某、陈某从事木马程序销售的情况下，仍受雇担任客户服务人员。被告人吕某、曾某二人因此各获利 32 万余元，严某、陈某共获利 31 万余元。

另指控，2008 年 3 月至 8 月底，被告人严某、张某、张某某分别垄断代理了“QQ 自由幻想”“QQ 华夏”“天龙八部”游戏的“温柔”木马程序，并通过姜某、汤某（均另案处理）等流量商将木马程序上传到网站，随玩家点击而植入玩家计算机系统，分别后台盗取“QQ 自由幻想”“QQ 华夏”“天龙八部”游戏账号、密码 82 780 组、427 717 组，后被告人严某将盗取账号、密码转卖给郑承勇、严盛伟（均另案处理）等人。

2008 年 3 月至 8 月间，被告人张某通过互联网从严某、陈某处垄断代理了“QQ 华夏”游戏的“温柔”木马程序。之后通过流量商任某、王某、林某、杨某、谢某（均另案处理）等人将木马程

序插入到各网站，随玩家点击而植入玩家计算机系统，后台盗取“QQ华夏”游戏账号、密码427 717组、2 449 591组。其中，被告人张某将所盗账号、密码转卖给他人，非法获利3万余元；被告人张某某采取同样手段非法获利23万余元。在被告人张某某传播木马程序过程中，被告人龚某为张某某联系租用了服务器，并在计算机系统内设置了能够存放窃取账号、密码的箱子，被告人陈建斌受雇于张某某，并按照张某某联系的买主将所盗账号、密码转卖他人，龚某非法获利2万元，陈建斌非法获利1万余元。

公诉机关认为被告人吕某、曾某、严某、陈某、丁某、许某、林某、张帆、张某某、龚某、陈建斌的行为已触犯了《中华人民共和国刑法》第二百八十六条第三款之规定，应当以破坏计算机信息系统罪追究其刑事责任，同时认为被告人吕某、曾某、严某、陈某造成的危害后果特别严重，其他被告人所造成的危害后果严重。

被告人吕某、曾某、严某、陈某、丁某、许某、林某、张某、张某某、龚某、陈建斌对公诉机关指控的犯罪事实均不持异议。

徐州市鼓楼区人民法院经审理查明：

1. 提供侵入计算机信息系统程序部分

2007年6月，被告人吕某、曾某开始开发用于盗取网络游戏账号、密码的木马程序，到2008年初该程序开发成功，并由曾某出面寻找合作伙伴帮助销售。2008年2月起，被告人严某接受曾某的委托，将该系列木马程序命名为“温柔”木马并总代理销售，同时按照不同网络游戏类型由吕某将该木马程序修改后分包给不同的一级代理商张某、张某某等人，并按照包用时间向后者收费，谋取非法利益。2008年6月，被告人陈某参与经营，与严某共同代理销售“温柔”系列木马程序。至案发前，吕某等人针对不同网络游戏类型开发并销售的“温柔”系列木马程序达28款，盗窃游戏账号、密码超过5 300 000组。被告人吕某、曾某二人共同获利645 780元，严某、陈某共获利31万元。

另查明，2008年6月中旬至7月底，被告人严某利用垄断“温柔”系列木马程序代理权之便，取得“QQ自由幻想”游戏的“温柔”木马程序使用权，然后通过姜某、汤某等人将该木马程序插入到正常网页，随游戏玩家点击网页而将木马程序植入玩家计算机系统，在玩家登录“QQ自由幻想”网络游戏时，木马程序自动运行并后台盗取游戏账号、密码合计82 780组，被告人严某将所盗取账号、密码转卖给郑承勇、严盛伟等人获取非法利益。

2008年4月至8月底，被告人丁某明知严某、陈某从事木马程序销售，仍在网络上受雇参与并担任售前客户服务，负责售前咨询和销售“温柔”系列木马程序，非法获利4 600元。

2008年7月初至7月底，被告人许某明知严某、陈某从事木马程序销售，仍参与并担任售后客户服务，负责售后技术问题咨询，非法获利2 000元。

2008年8月初至8月底，被告人林某明知严某、陈某从事木马程序销售，仍参与并担任售后客户服务，负责售后技术问题咨询。

上述事实有被告人吕某、曾某、严某、丁某、许某、林某、陈某、张某、张某某的供述，证人陈某、李某、黄某某、姜某、汤某、杨某、林某的证言，公安机关提供的相关网络银行账目、相关银行卡账目等书证，公安机关提供的电子证据检查笔录、远程勘验工作记录、电子数据检验鉴定书等证据予以证实。

2. 非法获取计算机信息系统数据部分

(1)2008年3月至8月间，被告人张某通过互联网从严某、陈某处获取了针对“QQ华夏”

网络游戏的盗号木马程序使用权。为了使该木马程序发挥盗号功能，通过流量商谢某、任某、汤某、杨某、林某、姜某等人将该木马程序插入到网络上各正常网页，随玩家点击而将木马程序植入玩家计算机系统，在上述玩家登录网络游戏时，木马程序自动运行并后台盗取“QQ 华夏”游戏账号、密码合计 427 717 组，被告人张某再将所盗账号、密码转卖给怀某等人，非法获利 3 万元。

上述事实有被告人张某供述，同案参与人严某、陈某的供述，证人谢某、任某、汤某、杨某、林某、姜某、陈某、唐某、怀某的证言，公安机关提供的电子证据检查笔录、远程勘验工作记录、电子数据检验鉴定书、相关银行卡账目等证据予以证明。

(2)2008 年 4 月至 8 月间，被告人张某某通过互联网从严某、陈某处获取了针对“天龙八部”网络游戏的盗号木马程序使用权。为了使该程序发挥作用，张某某以支付报酬的方式雇用被告人龚某为其租用了网络服务器，在计算机系统内设置了存放所窃取网络游戏账号、密码的箱子，以及提供其他技术支持。之后，被告人张某某通过流量商王某、杨某、谢某、任某、姜某等人将该木马程序插入到网络上各网页，随玩家点击相应网页而将该木马程序植入玩家计算机系统，在玩家登录“天龙八部”网络游戏后，木马程序自动运行并后台盗取“天龙八部”游戏账号、密码合计 2 449 591 组。在此期间，被告人陈建斌受雇于张某某，并按照张某某联系的买主将所盗账号、密码转卖他人。被告人张某某因此非法获利 23 万元，被告人龚某获利 2 万元，被告人陈建斌获利 1 万元。

上述事实有被告人张某某、龚某、陈建斌的供述，同案参与人严某的供述，证人王某、杨某、谢某、任某、姜某、叶某、何某、尤某某、林某、何某某的证言，公安机关提供的电子证据检查笔录、远程勘验工作记录、电子数据检验鉴定书、银行账目等证据证明。

另查明，2008 年 7 月 29 日，江苏省公安厅接到网民举报称徐州购物网(物理地址位于徐州市)病毒很严重。经过江苏省公安厅网警总队和徐州市公安局网警支队初查发现，徐州购物网网站上有 15 款可执行程序确定为网上流行的“温柔”系列木马程序，遂展开立案侦查。被告人严某、陈某、林某、丁某、许某于 2008 年 8 月 27 日晚被抓获归案；在严某、陈某、林某的协助下，公安机关于 2008 年 8 月 28 日将被告人曾某抓获归案；被告人张某、张某某、龚某某、陈某某也分别于 2008 年 8 月 28 日被抓获归案；被告人吕某于 2008 年 9 月 11 日被抓获归案，至此本案告破。

本案的争议焦点是：本案应定性为破坏计算机信息系统罪还是应认定为提供侵入计算机信息系统程序罪、非法获取计算机信息系统数据罪。

江苏省徐州市鼓楼区人民法院认为：

被告人吕某、曾某为了谋取非法利益，开发制作和提供用于窃取网络游戏账号、密码的系列木马程序达 28 款，被告人严某、陈某明知是盗号木马程序而予以代理销售，被告人丁某、许某、林某在代理销售过程中提供技术服务和帮助，上述被告人的行为情节严重，均已构成提供侵入计算机信息系统程序罪，且系共同犯罪。在共同犯罪中，作为木马程序制作者的吕某、曾某和负责代理销售系列木马程序的严某、陈某起主要作用，为主犯；丁某、许某、林某在代理销售系列木马程序犯罪中起次要、辅助作用，为从犯。

被告人张某、张某某明知是盗号木马程序而通过购买取得使用权后，借助他人技术手段加以传播，窃取网络游戏账号、密码数量巨大，情节严重；被告人龚某、陈建斌明知张某某通过非法手段获取游戏账号、密码而提供技术服务，情节严重，上述被告人的行为均已构成非法获取

计算机信息系统数据罪。在共同犯罪中，张某某起主要作用，系主犯；龚某、陈建斌受雇提供帮助，起次要、辅助作用，系从犯。

公诉机关指控本案11名被告人构成破坏计算机信息系统罪的公诉意见。经查，在刑法修正案(七)公布实施前对于故意制作、传播计算机病毒、木马等破坏性程序，影响计算机信息系统正常运行，后果严重的行为认定为破坏计算机信息系统罪。修正后增加的刑法第二百八十五条第二、三款对于制作、提供用于侵入计算机信息系统的木马程序以及利用传播木马程序获取他人存储、处理或者传输的数据，情节严重的行为，分别以提供侵入计算机信息系统程序罪和非法获取计算机信息系统数据罪论处，从而对于制作、传播木马程序以及利用木马程序非法获取他人数据的行为产生不同的法律界定。从本案被告人的主观方面看，无论是作为木马程序制作者的吕某、曾某，还是代理销售系列木马程序的严某、陈某(丁某、许某、林某系受雇服务于上述二人)，亦或通过传播木马程序获取他人账号、密码的张某、张某某(龚某、陈建斌受雇于张某某，为其提供技术或买卖服务)，其提供或传播木马程序的目的在于获取非法利益。从客观要件看，吕某、曾某制作、开发木马程序的行为和严某、陈某、丁某、许某、林某等人代理销售木马程序的行为符合修正后刑法第二百八十五条第三款规定的构成要件，表现为提供专门用于侵入计算机信息系统的程序；而张某、张某某等一级代理商及为之服务人员则符合该条第二款实行犯构成要件，属于违反国家规定利用技术手段获取计算机信息系统存储、处理、传输的数据，而数据则体现为上述所窃取的游戏账号、密码。另外，从制作、传播木马程序的客观危害看，主要体现在大量网络用户数据被非法获取，而无证据显示对计算机信息系统的正常运行造成其他直接危害结果。从刑法溯及力看，由于该案在刑法修正案(七)公布实施后进行审理，提供侵入计算机信息系统程序罪、非法获取计算机信息系统数据罪的基本法定刑轻于破坏计算机信息系统罪，适用修正后刑法第二百八十五条第二、三款的规定符合从旧兼从轻的原则。

综上，被告人吕某、曾某、严某、陈某、林某、陈某、丁某、许某以非法获利为目的，提供专门用于侵入、非法控制计算机信息系统的程序，造成严重后果，其行为已构成提供侵入计算机信息系统程序罪。被告人张某、张某某、龚某、陈建斌采用技术手段非法获取计算机信息系统中的数据，情节严重，已构成非法获取计算机信息系统数据罪。故公诉机关指控的犯罪事实清楚，但适用法律不当，予以纠正。

被告人曾某自愿认罪、主动退赃，被告人严仁海、陈某、林某协助公安机关抓获其他犯罪嫌疑人，具有一般立功情节，依法予以从轻处罚。被告人严某具有利用提供“温柔”系列木马程序之便，将其中一款木马程序通过他人传播到网页上进而非法获取他人数据的犯罪情节，故结合该情节对其所犯之罪酌情予以从重处罚。被告人丁某、许某、林某、龚某、陈建斌在提供侵入计算机信息系统程序或非法获取计算机信息系统数据共同犯罪中处于从犯地位，依法予以从轻处罚；被告人曾某案发后主动退出全部违法所得，酌情从轻处罚；被告人丁某、许某、林某归案后自愿认罪，确有悔罪表现，适用缓刑不致再危害社会，可以适用缓刑。

据此，徐州市鼓楼区人民法院依据《中华人民共和国刑法》第二百八十五条第二、三款、第十二条第一款、第二十五条第一款、第二十六条第一款、第二十七条、第六十八条第一款、第六十四条、第七十二条、第七十三条第二、三款之规定，于2009年12月15日作出(2009)鼓刑初字第150号刑事判决：

(1)被告人吕某犯提供侵入计算机信息系统程序罪，判处有期徒刑3年，并处罚金人民币