专 题 报 告

网络安全概述

李 昊，山秀明，任 勇
（清华大学电子工程系，北京 100084）

[摘要] 介绍了计算机网络安全问题所涉及的各方面内容。从全局角度介绍计算机网络安全的概念、体系结构和模型，讨论了网络安全主要包含的内容和研究方向，介绍当前网络安全的主要产品。

[关键词] 计算机；网络；系统；安全
[中图分类号] TP393 [文献标识码] A [文章编号] 1009－1742（2004）01－0010－06

现代信息化社会的发展，使得网络一词具有越来越重要的意义。网络与各种具体技术结合实现各自功能，如计算机网络（包括局域网、广域网、城域网、Internet 网）、电信网络（电话交换网（PSTN）、数字数据网（DDN）、帧中继网（FR）、ATM 网、X.25 网、ISDN 网、CHINANET 网等）、有线电视网（CATV 网）等。这里涉及的网络安全主要是指计算机网络的安全。

随着计算机网络规模的不断扩大以及新的应用（如电子商务、远程医疗等）不断涌现，威胁网络安全的潜在危险性也在增加，使得网络安全问题日趋复杂。对网络系统及其数据安全的挑战也随之增加。网络在使通信和信息的共享变得更为容易的同时，其自身也更多地被暴露在危险之中。网络安全问题往往具有伴随性，即伴随网络的扩张和功能的丰富，网络安全问题会随之变得更加复杂和多样，网络系统随时都会面临新出现的漏洞和隐患，所以网络安全问题是为保障信息安全随时需要考虑的问题。

通过对网络安全整体性描述、网络安全主要内容、网络安全主要研究方向及当前网络安全的主要产品 4 个方面的分析，对网络安全的概念、体系结构、结构模型、典型网络威胁、主要安全机制与服务、主要技术、主要安全标准与级别、安全协议、网络安全研究的理论基础、研究内容和方向、研究热点及主要安全产品等各个方面进行了讨论。

1 网络安全整体性描述

1.1 网络安全的概念

网络安全（计算机网络安全）是一个系统性概念，不仅包括计算机上信息存储的安全性，还要考虑信息传输过程的安全性。具体说来就是网络结点处的安全和通信链路上的安全共同构成了网络系统的安全，如图 1 所示。

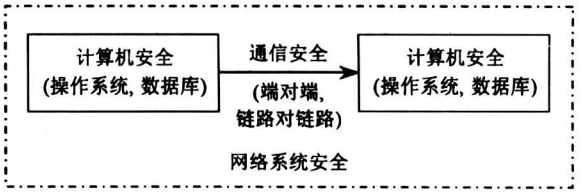

图 1 网络系统安全

Fig.1 Security of network system

因此网络安全的内容涵盖可以表述为：通信安全＋主机安全 →网络安全。事实上网络安全策略主要着重于系统的静态保护策略和系统不同部位动

[收稿日期] 2003－06－17；修回日期 2003－08－25
[基金项目] 国家自然科学基金重点资助项目（90204004）
[作者简介] 李 昊（1973－），女，天津市人，博士，清华大学博士后

态交换时的策略，其中动态交换保护策略是网络安全的重点。

网络中的计算机系统能够被攻击的 3 部分包括硬件、软件、数据。从概念上属于主机安全范畴，从拓扑上讲是网络结点安全。这也是安全措施重点保护的 3 部分。

网络安全从不同角度可以得到不同的划分。按照保护对象分，网络安全包含信息依存载体的安全问题和信息本身的安全问题。信息依存载体是指信息存储、处理和传输的介质，主要是物理概念，包括计算机系统、传输电缆、光纤及电磁波等[1]。信息载体的安全主要指介质破坏、电磁泄露、联网通信的截断、干扰和窃听等[2, 3]。信息本身的安全问题[2]主要指信息在存储、处理和传输过程中受到破坏、泄露和丢失等，从而导致信息的保密性、完整性和可用性受到侵害。因此网络安全按照受保护的对象可以分为硬体安全和软体安全，硬体安全指信息依存载体的安全，软体安全指信息本身的安全。这里讨论的重点是软体安全。

网络安全的目标是保密性、完整性、可用性[4]，有的文献中还增加了可靠性、真实性、不可抵赖性[5]、可审查性[6]等。保密性是网络信息不被泄露给非授权的用户、实体，以避免信息被非法利用的特性。保密性是在可靠性和可用性基础之上，保障网络信息安全的重要手段。常用保密技术包括防侦收、防辐射、信息加密、物理保密。完整性是网络信息未经授权不能进行改变的特性，即网络信息在存储或传输过程中保持不被偶然或蓄意地删除、修改、伪造、乱序、重放、插入等破坏和丢失的特性。完整性是一种面向信息的安全性，它要求保持信息的原样，即信息的正确生成和正确存储和传输。完整性与保密性不同，保密性要求信息不被泄露给未授权的人，而完整性则要求信息不致受到各种原因的破坏[5]。完整性与准确性也不相同，准确性是针对数据与现实世界的一致性而言，完整性强调的是数据本身的历史关系[4]。影响网络信息完整性的主要因素有设备故障、误码、人为攻击、计算机病毒等。保障网络信息完整性的主要方法有协议、纠错编码方法、密码校验和方法、数字签名、公证等[5]。可用性是网络信息可被授权实体访问并合法使用的特性。可用性还应该满足身份识别与确认、访问控制、审计跟踪、业务流控制等功能[5]。可靠性是网络信息系统能够在规定条件下和规定的时间内完成规定功能的特性。可靠性是系统安全的基本要求之一，是所有网络信息系统的建设和运行目标。网络信息系统的可靠性测度主要有：抗毁性、生存性和有效性。不可抵赖性也称作不可否认性，在网络信息系统的信息交互过程中，确信参与者的真实同一性，即所有参与者都不可能否认或抵赖曾经完成的操作和承诺[5]。利用信息源证据可以防止发信方不真实地否认已发送信息，利用递交接收证据可以防止收信方事后否认已经接收的信息[4]。可控性是对网络信息的传播及内容具有控制能力的特性[5]。

网络信息安全与保密的核心是，通过计算机、网络、密码技术和安全技术，保护在公用网络信息系统中传输、交换和存储的消息的保密性、完整性、真实性、可靠性、可用性、不可抵赖性等。

简言之，网络安全就是借助于一定安全策略，使信息在网络环境中的保密性、完整性及可用性(CIA)[7]受到保护，其主要目标是确保经网络传输的信息到达目的计算机后没有任何改变或丢失，以及只有授权者可以获取响应信息。因此必须确保所有组网部件能根据需求提供必要的功能。

需要注意的是安全策略的基础是安全机制，即数学原理决定安全机制，安全机制决定安全技术，安全技术决定安全策略，最终的安全策略是各种安全手段的系统集成，如防火墙、加密等技术如何配合使用策略等。

1.2　网络安全体系结构与安全模型

在开放式互联参考模型 OSI/RM 扩展部分，安全体系结构（security architecture）是指对网络系统安全功能的抽象描述，一般只从整体上定义网络系统所提供的安全服务和安全机制。事实上，安全体系结构不仅应该定义一个系统安全所需的各种元素，还应该包括这些元素之间的关系，以构成一个有机的整体[8]。安全体系结构主要包括安全服务、协议层次、实体单元等元素。文献[8]拓展了 OSI/RM 安全体系扩展部分关于安全体系的描述，并提出了一个三维安全框架模型，讨论了安全体系在工程中的应用。文献[9]提出一种主动 - 增强防御体系结构。

网络安全模型包括存取控制模型 Bell-LaPadula 模型，该模型定义了主体、客体、访问操作，用多级安全（MLS）的概念进行分级和标记，并采用了自主存取控制和强制存取控制的策略。此外还有

Clark-Wilson 模型和 Chinese Wall 模型[4, 10~12]，从学术角度对安全模型进行了研究。

1.3 网络安全结构模型

美国国防部（DOD）提出了“信息安全保障(information security assurance)”的概念，它由4部分组成，即防护（protect）、检测（detect）、反应（react）和恢复（recover），简称 PDRR 原则[13]。图2为 PDRR 模型。

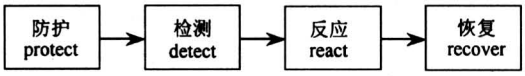

图2 PDRR 模型

Fig.2 Model of PDRR

2 网络安全主要内容

2.1 典型的网络威胁

网络威胁主要来源有恶意攻击、安全缺陷、软件漏洞、结构隐患等几个方面。人员有：内部人员(包括信息系统的管理者、使用者和决策者)；准内部人员（包括信息系统的开发者、维护者等)；特殊身份人员（具有特殊身份的人，比如，审计人员、稽查人员、记者等)；外部黑客或小组；竞争对手；网络恐怖组织；军事组织或国家组织等[14]。

典型攻击主要有：**a**. 拒绝接受服务（DOS)；**b**. 否定，某用户可能否认发送或接收某一事务处理或信息；**c**. 冒充，当攻击者冒充合法用户访问网络时，会给网络环境造成威胁；**d**. 修改；**e**. 重复播发；**f**. 窃听（网络监听)；**g**. 病毒侵害等[15~17]。黑客攻击使用的主要手法有缓冲区溢出、伪装 IP 攻击、利用安全“后门”等。

威胁产生主要原因有人为故意、偶然失误、自然灾害等。

黑客是网络威胁的主要制造者，其攻击的基本武器有扫描器（scanner)、嗅探器（sniffer)、口令攻击器（password cracker)、特洛伊木马、邮件炸弹（E－mail bomb)、病毒等。扫描器如 nessus，nmap，sscan，satan 等。嗅探器的英文写法是 Sniff，可以理解为一个安装在计算机上的窃听设备，它可以用来窃听计算机在网络上所产生的众多的信息。简单一点可以理解为一部电话的窃听装置，可以用来窃听双方通话的内容，而计算机网络嗅探器可以窃听计算机程序在网络上发送和接收到的数据[18]。嗅探器工具有如 sniffit，sunsniff 等。口令攻击器是使用诸如字典攻击等方法破解用户口令，工具如 John。特洛伊木马是一种黑客程序，它本身一般并不破坏硬盘上的数据，只是悄悄地潜伏在被感染的电脑里，被感染后攻击者可以通过因特网找到这台机器，在自己的电脑上远程操纵它，窃取用户的上网帐号和密码，随意修改或删除文件[19]，工具有“冰河”等。邮件炸弹就是向受害者发送大量垃圾邮件，由于邮箱容量有限，当庞大的邮件垃圾到达信箱的时候，就会把信箱挤爆，把正常的邮件冲掉。同时，由于占用大量的网络资源导致网络塞车[20]。已经有很多种能自动产生邮件炸弹的软件程序如 Nimingxin，QuickFyre，Amail，KaBoom，Emailbomb，Upyous 系列、雪崩等。计算机病毒主要指能够产生破坏的恶意代码，扩散速度和破坏能力都很大，如蠕虫等。

2.2 现有安全机制与服务

主要安全机制和服务有认证（authentication)、保密（confidentiality)、数据完整性（integrity)、访问控制（access control)、抗抵赖（non-repudiation）等。应该说安全机制是安全策略的基础，每一种安全策略都是安全机制的实现。

认证机制是要验证：第一，发送信息者是否真实，没有被冒充；第二，被发送信息是否真实，没有被窜改、重放、延迟，也就是信息认证和身份认证。保密机制的主要目的是防止没有合法授权用户获取信息。通过数学方法重组数据，将明文转换成密文，只有经过解密才能将密文变回明文，恢复成可用信息。访问控制就是控制相应级别的用户使用相应级别的权利，如读、写、执行不同的操作，由不同权限的用户掌握。抗抵赖机制就是防止行为的否认。

2.3 网络安全主要技术

每一种安全服务和机制有可能由不同种的安全技术来实现，每一种安全技术也有可能为不同的安全策略所用。

认证方式一般包含两种：一种是第三方信任；另一种是直接信任，以防止信息被非法窃取或伪造。认证主要解决3个问题：你了解什么（了解密码)，你有什么（用户持有智能卡、Java 卡)，你是谁（生物统计学，如指纹、虹膜鉴别)，如密钥认证、数字签名（基于杂凑算法)、生物识别等技术。

访问控制技术包括包过滤技术、代理服务技术、复合型技术、审计技术、路由器加密技术。

数据完整性技术可采用数据备份和恢复等。

加密技术种类繁多，它是保障信息安全最关键和最基本的技术手段和理论基础。常用的加密技术分为软件加密和硬件加密，两种方法各有其所长。对称密钥（包括分组密码和流密码）即加密和解密使用同样的密钥，目前有 DES 算法、三重 DES 算法、IDES 算法，AES 算法，缺点是密钥长度短、密码空间小，“穷举”方式进攻的代价小，它的机制就是采取初始置换、密钥生成、乘积变换、逆初始置换等几个环节。非对称密钥加密方法加密和解密使用不同密钥，即公开密钥和秘密密钥。公开密钥（公钥）用于机密性信息的加密；秘密密钥（私钥）用于对加密信息的解密。主要有 RSA 算法、DH 算法、ECDH 算法[21]，其优点在于易实现密钥管理，便于数字签名，不足之处是算法较复杂，加密解密花费时间长。从目前实际的安全防范应用中，尤其是信息量较大、网络结构复杂时，通常采用对称密钥加密技术。为了防范密钥受到各种形式的黑客攻击，如基于 Internet 的联机运算，即利用许多台计算机采用“穷举”方式来破译密码。因此，密钥的长度越来越长。目前一般密钥的长度为 64 b，128 b，实践证明它是安全的，同时也满足计算机的速度。

抗抵赖性的实现可以采用数字签名技术等。

此外，在具体应用中还有扫描评估、信息的分析与监控、防病毒保护、安全管理、网络安全检测等。

在信息网络建设中一般采取许多安全措施的集成，如物理安全、防火墙、网络安全扫描评估系统、系统安全扫描评估系统、信息流捕获分析系统、安全实时监控系统、漏洞扫描技术、入侵检测与实时响应系统、网络病毒防护系统、访问控制及信息的加密系统。各种技术和措施的恰当综合使用，才能达到网络整体安全的目标。

2.4　网络主要安全标准、级别与组织

迄今尚未形成有关 Internet/Internat 安全体系的完整理论，难以制定统一的安全政策，目前较为普遍接受的安全理论和标准主要为 CEC 的《信息技术安全评级准则》、NCSC 的《可信网络指南》、ISO 的 ISO7498－2 等。

美国国防部所属的国家计算机安全中心（NCSC）提出了网络安全性标准（DoD5200.28－STD），即可信任计算机标准评估准则（Trusted computer standards evaluation criteria），也叫橘皮书（Orange book）扩展而成的《可信网络指南》，把可信网络的安全性由低到高分为四类七级，分别是：D 级，安全保护欠缺级；C1 级，自主安全保护级；C2 级，受控存取保护级；B1 级，标记安全保护级；B2 级，结构化保护级；B3 级，安全域级；A1 级，验证设计级。认为要使系统免受攻击，对应不同的安全级别、硬件、软件和存储的信息应实施不同的安全保护。安全级别对不同类型的物理安全、用户身份验证（authentication）、操作系统软件的可信任性和用户应用程序进行了安全描述，标准限制了可连接到主机系统的系统类型。

数据加密的标准化工作开始很早，1976 年美国国家标准局颁布了“数据加密标准算法（DES）”。1984 年，国际标准化组织 ISO/TC97 决定正式成立分技术委员会，即 SC20，开展制定信息技术安全标准工作。后 ISO 撤消原来的 SC20，组建新的 SC27，并在 1990 年 4 月瑞典斯德哥尔摩年会上正式成立 SC27——信息技术－安全技术。SC27 的工作范围是信息技术安全的一般方法和信息技术安全标准体系，包括确定信息技术系统安全服务的一般要求、开发安全技术和机制、开发安全指南、开发管理支撑文件和标准[22]。与加密相关的协议还有 PKCS（Public-key cryptography standards），SSL（Secure soket layer）handshake protocol，S－HTTP（Secure hypertex transfer protocol），PTC（Private communication technology）Protocol，S/WAN（Secure wide area network），SET（Secure electronic transaction），S/MIME（Secure/Multipuopose internet mail extension）[23]。

国内主要是等同采用国际标准。主要有由公安部主持制定、国家技术标准局发布的中华人民共和国国家标准 GB17895－1999《计算机信息系统安全保护等级划分准则》。该准则将信息系统安全分为 5 个等级，分别是自主保护级、系统审计保护级、安全标记保护级、结构化保护级和访问验证保护级。主要的安全考核指标有身份认证、自主访问控制、数据完整性、审计、隐蔽信道分析、客体重用、强制访问控制、安全标记、可信路径和可信恢复等，这些指标涵盖了不同级别的安全要求。此外，针对不同的技术领域还有其他一些安全标准，如《信息处理系统开放系统互联基本参考模型：第二部分 安全体系结构》（GB/T 9387.2 1995）、《信

息处理 数据加密 实体鉴别机制：第一部分 一般模型》(GB15834.1－1995)、《信息技术设备的安全》(GB4943－1995)[22]、GB9361－88 计算机场地安全要求、GB15851－1995 信息技术（安全技术(带消息恢复的数字签名方案等。国内军用标准有：GJB1281－91《指挥自动化计算机网络安全要求》，GJB1295－91《军队通用计算机系统使用安全要求》，GJB1894－94《自动化指挥系统数据加密要求》等[23]。

国际标准和机构还有国际电报和电话咨询委员会（CCITT，Consultative Commit Internal Telegraph and Telephone）的V系列和X系列建议书。电气和电子工程师学会（IEEE，Institute of Electrical and Electronic Engineers）制定的P1363公开密钥密码标准。国际信息处理联合会第十一技术委员会（IFTP TC11），Internet体系结构委员会(IAB)，美国国家标准协会（ANSI），美国国家标准局与美国商业部国家技术标准研究所（NBS和NIST)，美国电子工业协会（EIA）等组织均在从事与信息安全有关的工作[23]。

2.5 网络主要安全协议

网络安全协议主要包括：网络层协议——IPsec（包括认证头协议AH，封装安全载荷协议ESP)；安全套接口层（介于传输层和应用层之间）——SSL；应用层协议——安全电子交易(SET）协议、安全多用途Internet邮件扩展（S/MIME)、PGP（Pretty good privacy）加密等[23]。

1996年IETF开发的IPsec（Internet Protocol Security）是一个用于保证通过IP网络进行安全秘密通信的开放式标准框架。IPsec实现了网络层的加密和认证，提供端到端的安全解决方案。IPsec联合使用多种安全技术，包括两种协议，一个是认证头（AH，authentication header）协议，另一个是封装安全载荷（ESP，encapsulating security payload）协议。IPsec有2种模式：传输模式和隧道模式[21]。

1994年Netscape最先提出的安全套接字协议层SSL是一种基于会话、加密和认证的Internet协议，目的是在两实体（客户和服务器）之间提供一个安全的通道。

安全电子交易（SET，secure electronic transaction）为保护在Internet电子商务交易中使用的支付卡免遭欺诈提供了框架。SET通过保证持卡人数据的保密性和完整性及一种认证机制来保护支付卡[21]。

2.6 安全产品种类

安全产品是各生产厂商制作好的有特定安全功能的产品，主要种类有防火墙（firewall)、VPN(虚拟专用网)、扫描器（scanner)、入侵检测系统(IDS，intrusion detection system)、SVN（安全虚拟网络结构)、密码机、防毒软件、安全网关、网络流量分析产品以及各种各样的整体解决方案等。

3 网络安全的研究

网络安全从本质上讲属于信息安全，凡是涉及到信息的保密性、完整性、可用性、真实性和可控性相关技术和理论都是安全的研究领域，是一门涉及计算机科学、网络技术、通信技术、密码技术、信息安全技术、应用数学、数论、信息论等多种学科的综合性学科。

3.1 网络安全的理论基础

网络安全的研究很多刚处于起步阶段，希望达到以一种严格的形式化描述来作为某种安全机制的内核，但现在大部分技术却没有这样的理论依据。这也是今后工作应该努力的目标。在安全机制中，相对数学原理而言，加密机制是最为严格的一种安全机制，如公钥算法使用了数论中的大素数分解理论，消息摘要MD5或SHA－1算法使用了杂凑函数（HASH函数）方法，密钥管理中使用了门限原理等。再比如IDS中的特征识别采用统计分析、模式识别等方法。网络安全研究上的突破归根结底还是要在基础理论上有所突破，无论是研究加密算法还是信息的统计分析方法均需要严格的理论基础，因此进行基础理论研究是今后的重点。

3.2 网络安全的研究内容和方向

1）*安全基础核心技术* 密码算法标准及其高速芯片实现技术，公钥基础设施PKI关键技术、信息系统平台安全核心技术等等。

2）*网络环境安全应用技术* 密钥管理和交换技术等等。

3）*安全综合防御关键技术* 大规模入侵检测与战略预警技术，应急响应和事件恢复技术，网络信息内容分析与监控技术，网络病毒防治技术，信息安全积极防御技术等等。

4）*信息安全新技术* 密码新技术与应用研究，安全体系结构研究，安全协议研究等等。

3.3 当前研究热点与发展方向

当前关于网络安全的研究热点主要包括新型加密技术、入侵检测 IDS、病毒识别与清除技术、设备电磁泄漏防护技术、数据恢复技术、基于新理论的密码新技术等，以及 VPN 和防火墙等应用层次技术产品研究。

此外以量子通信为代表的量子密码技术成为保密通信的发展热点，为网络安全通信带来了光明。

4 国内外网络安全主要产品

国外主流厂商主要有 Network Associates（美国网络联盟，主要产品 Sniffer），Symantec（赛门铁克，世界第一大软件供应商，主要产品 Norton.，SES 等）、网络安全行业标准的拥有者——以色列 Check Point 公司（互联网安全解决方案 Check Point Next Generation）、iS－One 安氏、Cisco（思科）、网屏、冠群、NetScreen 等，诺基亚和微软也在进军安全产品市场。国内主要厂商：联想、东软、瑞星、天融信、启明星辰、东软股份、上海格尔等。目前，国内的防火墙产品中，国外厂商占 60 %，国外主流厂商为 Cisco，CheckPoint，NetScreen 等，国内主流厂商为东软股份、天融信等。而在入侵监测与评估软件中，国外占 70 % 以上，国内不足 30 %，国外的主流厂商为安氏，及 ISS 公司（国际互联网安全系统公司）的 Real Secure，NAI 公司的 CyberCop Monitor，Axent 公司的 NetProwler，Cisco 公司的 Netranger，CA 公司的 Sessionwall－3 等，国内厂商有启明星辰、东软股份、上海格尔、天融信等。用户在购买安全产品时，对于防火墙，选择 Cisco 公司的最多，其次是 CheckPoint 和东软股份；对于防病毒产品，选择 Symantec 的最多，其次是瑞星和冠群金辰。此外 CheckPoint 占据着全球网络安全解决方案 42%的市场份额，其中在 VPN 虚拟专用网中所占的份额高达 62 %。IDS 主要产品：典型代表是 ISS 公司（国际互联网安全系统公司）的 RealSecure，NAI 公司的 CyberCop Monitor，Axent 公司的 NetProwler，CISCO 公司的 Netranger，CA 公司的 Sessionwall－3 等，国内的该类产品较少，但发展较快，已有总参北方所、中科网威、启明星辰、北京理工等公司推出的产品。

5 结语

计算机网络安全问题是伴随计算机网络发展不可忽视的问题，只有更好地解决好这一问题，网络才能更加稳步快速地发展，从而提供更加快捷可靠的网络服务。因此，除了对网络安全问题给予足够的重视之外，要从安全基础理论、安全机制、安全技术、安全策略、安全产品等各个层面进行深入细致的研究，才能更好地实现网络的安全和保护，即只有进入到网络安全涉及的每一层面，同时把握安全问题的全局性才能更好地实现网络的保密、完整及可用性。

参考文献

[1] 林晓焕，林　刚. 数字地球下的网络信息安全问题研究 [J]. 现代计算机，2001，(9)：44～51

[2] 何红波，王文军. 大型计算机网络系统的安全控制 [J]. 电子对抗技术，2000，15 (3)：44～48

[3] 胡西川. 维护网络硬件设施保障系统安全运行 [J]. 电子质量，2003，(2)：100

[4] Schneier B. Secrets and lies－digital security in a networked world [M]. New York：John Wiley Press，2000

[5] 网络安全的目标 [EB/OL]. http：//xexploit. css. com. cn/ghost/aqjd/content/a16. htm，2003－08－19

[6] 吴会松. 网络安全讲座 [J]. 中国数据通讯网络，2000，(2)：46～51

[7] 陈修环，石　岩. 计算机网络安全管理 [J]. 小型微型计算机系统，1999，20 (5)：343～346

[8] 段海新，吴建平. 计算机网络安全体系的一种框架结构及其应用 [J]. 计算机工程与应用，2000，(5)：24～27

[9] 董永乐，史美林，张信成. 主动－增强防御体系结构及其在 CSCW 中的应用 [EB/OL]. http：//cscw. cs. tsinghua. edu. cn/cscwpapers/dyle/ Paper_for_mag. doc，1999－06－08

[10] 卿斯汉. 网络安全检测的理论和实践 (一) [J]. 计算机系统应用，2001，(11)：24～26

[11] Brewer D，Nash M. The Chinese Wall Security Policy [A]. IEEE Symposium on Security and Privacy [C]. IEEE：Computer Society Press，1989

[12] Millen J K. Models of multilevel computer security [J]. Advances in Computrs，1989，(29)：1～45

[13] 蒋　韬，李信满，刘积仁. 信息安全模型研究 [J]. 小型微型计算机系统，2000，21 (10)：1078～1080

[14] 网络安全威胁的主要来源 [EB/OL]. http：//www0. ccidnet. com/news/gl/2001/06/01/54_48727. html，2001－06－01

(下转第 73 页)

Research of Glasses Forming Ability of Bulk Metallic Glasses Based on Kinetics

Cai Anhui[1], Pan Ye[1], Sun Guoxiong[1], Ruan Xuping[2]

(1. *Department of Mechanical Engineering, Southeast University, Nanjing* 210096, *China*;
2. *Department of Physics, Loudi Normal College, Loudi, Hunan* 417000, *China*)

[**Abstract**] The key step of exploiting new type BMG is to judge quickly the glass forming ability (GFA) of bulk metallic glasses (BMG). The reliability and limitation that T_{rg} was suited for judging of the GFA of BMG was made clear by using dynamics based on the addition principle in this paper, and the theory basis was provided for making BMG. The minimum of T_{rg} for forming the BMG was 0.406 6, at the same time, two theory optimum T_{rg}, i.e. $T_{rg}=1$, $T_{rg}=0$, were obtained. A new parameter (CPS) for judging the magnitude or the smooth and stability of GFA of BMG was put forward, the magnitude of GFA of BMG was calculated by using it. The result of sequence of GFA of BMG was unanimous to Inoue's. At one time, the results were examined according to the average variance of Z_{max} and R_c of BMG, and all results were measured with one another. The magnitude of ΔH_{mg} was a feasible method for quickly appraising the capacity and stability of GFA of BMG.

[**Key words**] kinetics; bulk metal glasses; glass forming ability; addition principle; stability

(上接第 15 页)

[15] 刘　琦. 网络安全的脆弱性及常见攻击手段[J]. 公安大学学报, 2001, 22(22): 17～19

[16] 金　雷,谢　立. 网络安全综述[J]. 计算机工程与设计, 2003, 24(2): 19～22

[17] Paulson L D. Wanted : more network-security graduates and research[J]. Computer, 2002, 35(2): 22～24

[18] 嗅探原理与反嗅探技术详解[EB/OL]. http://www.xfocus.net/articles/2001 10/279.html, 2001－10－16

[19] 解读特洛伊木马[EB/OL]. http://tech.tyfo.com/tech/block/html/2001070 400248.html, 2001－07－04

[20] 电子邮件炸弹攻防[EB/OL]. http://elvishua.myetang.com/wlsafe/aqcl/03.htm, 2003－06－05

[21] Burnett S, Paine A. CRYPTOGRAPHY 密码工程[M]. 冯登国. 北京:清华大学出版社, 2001

[22] 安全标准与体系[EB/OL]. http://www.ihep.ac.cn/security/lanmu/biaozhun, 2003－08－20

[23] 赵战生, 冯登国, 戴英侠, 等. 信息安全技术浅谈[M]. 北京:科学出版社, 1999

Summarization of Network Security

Li Ying, Shan Xiuming, RenYong

(*Department of Electronics Engineering of Tsinghua University, Beijing* 100084, *China*)

[**Abstract**] The content of computer network security is discussed in this article. Firstly, the concept, system and structure and model of computer network security are given. Then the main content and correlative researching aspect are included. In the end, the main product is introduced.

[**Key words**] computer; network; system; security