英汉信息安全技术辞典

ENGLISH-CHINESE DICTIONARY OF INFORMATION SECURITY TECHNOLOGY

主编 胡苏太 董立平 柴亚利

国防工业出版社
National Defence Industry Press http://www.ndip.cn

英汉信息安全技术辞典

ENGLISH-CHINESE DICTIONARY OF INFORMATION SECURITY TECHNOLOGY

主编　胡苏太　董立平　柴亚利

国防工业出版社

·北京·

图书在版编目(CIP)数据

英汉信息安全技术辞典/胡苏太等主编.—北京:国防工业出版社,2004.8
ISBN 7-118-03349-9

Ⅰ.英... Ⅱ.胡... Ⅲ.信息系统-安全技术-词典-英、汉 Ⅳ.TP309-61

中国版本图书馆 CIP 数据核字(2003)第 118072 号

国防工业出版社出版发行
(北京市海淀区紫竹院南路 23 号)
(邮政编码 100044)
腾飞胶印厂印刷
新华书店经售
*
开本 850×1168 1/32 印张 17 731 千字
2004 年 8 月第 1 版 2004 年 8 月北京第 1 次印刷
印数:1—5000 册 定价:39.00 元

《英汉信息安全技术辞典》
编辑委员会

序

信息是现代社会的重要战略资源，国际上围绕信息的获取、控制和利用的斗争日益激烈，世界各国越来越认识到信息安全的重要性，采用各种安全技术和管理措施，加强信息安全。随着我国计算机技术和因特网的发展，信息安全问题也日益成为人们关注的焦点。

信息安全是一门综合性技术学科，它与众多学科有着密切联系，如数学、物理、通信、计算机、密码学、系统工程、管理科学等等。随着信息技术的发展与应用，信息安全的内涵在不断延伸。从最初的信息保密性，扩展到信息的完整性、可用性、可控性和不可否认性，继而又发展为攻(攻击)、防(防范)、测(检测)、控(控制)、管(管理)、评(评估)等多个方面。

《英汉信息安全技术辞典》牢牢地把握信息安全技术的发展方向，对近几年新出现的信息安全方面的名词、术语、字符和缩略语做了广泛的搜集，辞典词条定义清楚、释义确切、用词规范，是一部符合时代需求、具有专业特色的新辞书。

我深信，《英汉信息安全技术辞典》的编辑出版，为普及信息安全知识，提高信息安全意识做了一件扎扎实实的富有意义的工作，对我国信息安全事业的发展必将产生积极的影响。

中国工程院院士 周仲义

2003 年 8 月

前　言

随着全球信息化的飞速发展，信息革命和计算机在社会各个层面的应用使人类生活发生了翻天覆地的变化。信息已成为代表综合国力的战略资源，成为国民经济快速发展的基础。与此同时，信息安全也受到越来越多的关注，它直接关系到国家的安全，已成为国民经济能否健康有序发展的保证。

信息安全是一门技术性、实用性很强的综合学科，它与众多学科有着密切联系，如数学、物理、通信、密码学、信息管理、工程技术和计算机等等。随着信息技术的发展与应用，信息安全的内涵在不断的延伸，从最初的信息保密性发展到信息的完整性、可用性、可控性和不可否认性，进而又发展为“攻（攻击）、防（防范）、测（检测）、控（控制）、管（管理）、评（评估）”等多方面的基础理论和实施技术。

近几年，信息安全产业飞速发展，世界安全产品市场每年增长25%左右，我国信息安全市场保持每年翻一番的发展速度。预计到2006年，世界安全产品市场将达到1550亿美元。

信息安全技术和产品的发展日新月异，伴随而产生了许多新知识、新术语、新词汇，并广泛地频繁出现在书报、杂志上。为了有助于关注信息安全的人士全面深入地了解和掌握相关技术知识和发展情况，便于广大用户和读者理解与应用这些新术语、新词汇，国防工业出版社组织编纂了《英汉信息安全技术辞典》。

辞典尽可能对近几年新出现的关于信息安全方面的名词、术语、字符和缩略语做了全面搜集和释义，突出新、特、全，内容涵盖信息安全机制、密码技术、安全服务、安全管理、安全法规政策、信息战、安全工具、安全机构、通信及网络安全等有关名词、术语、字

符和缩略语，共收录词条 7000 余条。同时，辞典中还收录了有关信息安全的缩略语汇编、国内外安全法规汇编、国外信息安全机构简介和信息安全工具、程序等，供读者查阅使用。

希望本辞典成为广大读者喜爱的工具书。由于编纂时间仓促及水平有限，错误在所难免，敬请广大读者批评指正。

《英汉信息安全技术辞典》编委会

2003 年 7 月

使用说明

1. 本辞典的词条按其英文字母(不分大小写)排序,括号中的英文字母不参加排序。具体情况说明如下:

(1) 以数字、符号开头的词条另立一个(数字)部,以#为标记,排于英文词部之后。

(2) 词条中带连字符和"&"的词汇,按各自的独立词汇排序(例如,end-entity 当作 end 和 entity 两个词排序)。为便于查阅,对以下词条 on-line 视为 online;non-这类复合词视为 nonXX 排序。

(3) 词条中的其他符号[如圆点(Net. abuse)、斜杠(A/UX)、*(. * rc)、$($HOME)、=(P = NP problem)等分别按 Netabuse、AUX、rc、HOME 及 PNP problem 排序],原则上不参加排序。

(4) 除上述(1)的情况之外,词条中含有数字的(如 T1、T2 等),则按数字大小为序。

2. 英文术语的译名以科学性和实用性相结合的原则,尽量表达其内涵,而非取其字面意义。术语的中译名若有多个意义、意义相同或相近者,用逗号(,)分开;若意义不同,则用(;)分开。

3. 释义中,圆括号( )中的内容是解释、注释、或可取可舍。

4. 词条中除正常解释外,还有见和参见 XX 词条。这些词条在本辞典中可以找到相应的解释。

5. 为方便广大读者充分利用有关信息安全方面的丰富资源,在正文之后编纂了附录,以供读者查阅。

目　录

A a

A1　可验证的安全设计级　A1 级称为可验证的安全设计级，是桔皮书(美国国防部《可信计算机系统评估准则》DOD 5200.28-STD)中定义的最高可信等级。它包含了一个严格的设计、控制和验证过程。A 级包含了较低级别的所有特性。

A3 algorithm　A3 算法　一种用于 GSM 蜂窝电话的 IMSI(国际移动用户号)认证算法。

A5 algorithm　A5 算法　A5 算法是一种加密密钥生成算法，它是整个欧洲和美国 GSM 蜂窝电话所使用的一种保护数字蜂窝电话通信的密码算法。

A8　algorithm　A8 算法　一种用于 GSM 蜂窝电话的用户密钥生成算法。

AAA　3A 标准　AAA 是 Authentication、Authorization、Accounting 的简称，指防火墙的认证、授权、统计功能。其中，认证提供对用户的合法性检查；授权用于规范每个用户的行为；统计是对每个用户的跟踪记录。在结合了 3A 功能的防火墙中，用户经由防火墙提供服务时，必须先经过认证和授权，同时其行为都将被日志记录。

AAFID　自治代理入侵检测系统　AAFID 是 Autonomous Agents for Intrusion Detection 的缩写。它是美国 Purdue 大学于 1999 年设计的分布式入侵检测系统。其采用分布式部件进行数据收集，各部件采用层次结构形式；检测是在各自的主机上进行，并且相互之间可以交换信息，在检测到入侵时采取响应。AAFID 系统主要包含四个部件：监视器(Monitor)、收发器(Transceiver)、代理(Agent)和过滤器(Filter)。

ABA Guidelines　ABA 指南　美国条形码协会(ABA)数字签名指南，它是电子商务中使用数字签名和数字证书的法定准则。

abandonware　取消件　指不再由原创公司销售或分发，但仍能从其他来源获得的计算机软件，如操作系统、字处理程序、交互式游戏或音频文件等。

ability to add attributes　增加属性能力　某些数字签名技术具有的一种能力，例如，增加一个时间戳(作为数字签名的一部分)的能力。

absolute path　绝对路径　指定的资源绝对路径，从根目录开始。

abstract syntax　抽象语法　一种不受应用程序或平台限制的语法(构成命令的规则)。

Abstract Syntax Notation One(ASN.1)　抽象语法标号 1　一种 OSI 语言，用于 Internet 基础结构一部分的简单网络管理协议(SNMP)编码。

abuse　滥用　指计算机用户进行非授权的或者禁止的活动。

ACAP　应用程序配置访问协议　ACAP 是 Application Configuration Access Protocol 的缩写。ACAP 是远程服务器访问程序配置信息的标准，它允许任何一个工作站的用户通过在中心服务器上读写数值来使用和改变它们的配置。

ACC　访问控制中心　见 Access Control

Center。

acceptable risk　可接受风险　一次结论为"一个系统或一项活动满足政策规定的最低限度的安全要求"的评估。它用于风险分析中。

acceptable use　可接受使用　Internet服务提供商要求其所有用户皆同意可接受使用Internet和Usenet资源的一些规则。不同服务提供商的可接受使用策略互不相同。

acceptance criteria　验收准则　软件产品成功地完成某一测试阶段中的工作所必须满足的准则，或软件产品满足交货要求的准则。

acceptance inspection　验收审查　确定一项设备和系统是否符合特定的技术和性能标准的最终审查。这一审查应在设备和软件测试完成后立即进行，是信息系统投入试运行或被接收的前提条件。

acceptance review　验收评审　软件开发工作的重要步骤之一。验收评审包括"检查点/冻结点"评审和介绍性评审。

acceptance testing　验收测试　软件开发工作中测试阶段的步骤之一。在系统测试完成之后再进行验收测试，而且要让用户参加。因为验收测试时完全根据说明书来测试，故应假定对程序的内部结构毫无所知，即把程序看为一个黑盒子。测试时应在常规的、强化的和退化的条件下，用模块操作来检验程序。所有的软件包都应检验。与实现的有效性及其限制条件有关的信息应记录下来，以供维护人员在维护期间参考。

access　连接；访问方式；访问能力；访问　1. 与Internet的一种连接。2. 访问Internet的方式（网络访问、拨号访问等）。3. 执行某些活动或读取特权信息的能力。4. 使用某一信息系统资源的机会。

access authorization　访问授权　授予一用户、程序或工作站使用某类程序或数据的权利。

access category　访问类别　根据信息系统中被授权访问资源或资源组而规定的用户、程序、数据或进程等的等级。

access control　访问控制　对信息系统资源的访问进行限制，使之只能让获得授权的用户、程序、过程或其他系统访问。

Access Control Center（ACC）　访问控制中心　一台包含了一个数据库的计算机，数据库中的项定义了一种访问控制服务的安全策略。ACC有时与一个密钥中心协调使用，以在一个密钥分布系统中实现访问控制。

Access Control List（ACL）　访问控制表　计算机保密系统中与某现场相关联的一种表，是在主体与客体之间实现自主访问控制和/或强制访问控制的机制。它标识授权访问该现场的所有主机及其访问权利。

access control mechanism　访问控制机制　一个信息系统中为检测和拒绝未授权访问并允许授权访问而设计的安全保护措施。

Access Control Officer（ACO）　访问控制官　负责对信息系统资源访问进行限制的指定人员。

access control service　访问控制服务　访问控制服务就是对某一些确知身份，限制对某些资源的访问。访问控制服

务可以防止未授权的实体访问资源(如计算机资源、信息资源等),所谓未授权的访问就是未经授权的使用、修改、销毁以及颁发指令等。访问控制服务一般要与不同的安全策略协调一致。访问控制服务直接支持保密性、完整性、可用性和认证的安全性能,其中对保密性、完整性和认证所起的作用十分明显。对于可用性所起的作用,取决于对其他一些方面是否有效地控制。

access establishment 建立访问 指安全策略和规则的确立,用于确定某个实体对一个终端、交易、程序或过程的初始访问权。

access level 访问等级 安全等级中的分级分类部分,用于识别信息系统数据的敏感程度和用户得到的许可或授权范围。访问等级和各种不分级类别共同组成客体敏感标志。

access list 访问表 1.(信息系统中)一种汇编,它包括各种用户、过程及各自授权进行的访问等级和类型。2.(通信安全中)经批准允许进入受控区域的人员名单。

access method 访问方法 用于确定任意时刻,哪个网络结点能访问传输介质的一组规定。

access mode 访问模式 计算机系统中的主体对客体所能够执行的一种显式数据处理操作,如读、写、添加或执行。

access modification 访问修改 指安全策略和规则的确立,用于决定对某个实体访问一个终端、交易、程序或过程的权利进行修改的类型或原因。

access number 访问号码 需要连接一个布告栏系统和在线服务机构时所拨的号码。

access period 访问周期 访问权的有效时间段,一般用天数或星期数来表示。

access port 访问端口 一个逻辑或物理标识符,计算机用它来识别不同的终端输入/输出数据流。

access privileges 访问特权 授权使用的一种专用访问级。

access profile 访问范围 每个用户所能访问的受保护客体一览表。

access protocol 访问协议,访问规程 各工作站在共享的网络介质上发送信息时,为避免冲突而使用的规则集合,也称为"介质访问控制协议(media-access control protocol)"。

access provider 访问提供者 一种提供Internet访问的机构,如Internet服务提供商、大学或雇主。

access right 访问权限 指授予一个进程的对某一特定对象的访问方式。不同的访问权限支持不同的对象,访问权限存入该对象的访问控制表(ACL)中。

access rule 访问规则 访问规则规定若干条件,在这些条件下可准许访问一个资源。一般地讲,规则使用户和资源配对,然后指定该用户可在该文件上执行哪些操作,如只读、不许执行或不许访问。由负责实施安全政策的系统管理人员来应用这些规则。这些规则可以用一个访问控制模型来表示。硬件或软件的安全内核部分负责实施这些规则,并将企图违反规则的行为报告给审计系统。

access server 访问服务器 为远程用户提供访问服务的一台计算机。远程用户通过调制解调器连接到系统访问网络资源,就好像其计算机直接连接到网络上一样。

access sharing 访问共享 允许两个或多个用户同时访问一个文件或设备。

access site 访问站点 指在 Internet 网上,可使用电话线连接方式访问的主机系统,该主机系统为一个地区的用户提供通过电话线的网络服务。

access time 访问时间 1. 从提出对磁盘或内存的访问要求,到信息到达提出访问的装置之间的时间周期。内存访问时间是指数据从内存传到处理器(或相反)所需的时间。磁盘访问时间是指将读/写头移到要访问的数据上所花的时间。内存访问时间一般小于 80ns,硬盘访问时间一般小于 18μs。2. 用户可以访问特定对象或资源的时间段。例如,管理员可能会限制用户只能在工作日的上午 8 点到下午 5 点登录,这就是用户的访问时间。

access token 访问令牌 一种包含了对一个用户或一个组织的授权信息的数据结构。系统利用访问令牌来控制对安全的访问,并且对用户在本地计算机上执行各种与系统相关操作的能力进行控制。

access type 访问类型 对客体实施操作的特权。读、写、执行、添加、修改、删除和创建等都是访问类型的事例。

accessibility privileged policy 可接受特权策略 特权应用时必须使用的策略。可接受特权策略指定了在验证特权的过程中必须使用的策略集合。

accessible space 可见空间 用户能掌握所有人员进出情况的区域。在该区域内,不可能有机会进行隐蔽的 TEMPEST 监视,并且可以界定出最接近潜在车载 TEMPEST 截收活动的地点。

accessory virus 附件型病毒 病毒以附件的形式进行伪装,只要用户执行或打开附件中的文件,就会受到病毒的感染。这种类型的病毒基于 JavaScript、VBScript、Java 实现的居多,如爱虫病毒、梅利莎病毒等。

accessware 安全访问程序 该程序是确保和提高安全访问的一种网络安全程序。它是建立一个安全的内部或外部网络所需的,它可将访问控制、信息保密、用户名、数据整体性和信息管理等有机地结合起来。

AccessWatch 访问监控程序 该程序用于特定的网站综合观察每天的活动和网站传输状况。它每小时将服务器的负载、网页请求、域和主计算机访问等产生一份统计报表。访问监控程序使用图形化、易读的压缩格式显示结果。这一程序在 Unix 平台上运作。

accidental data 故障数据 在信息系统中,有些表中的数据并不要求具有特定值,因而用问号(?)代替。称此类数据为故障数据。设定故障数据的目的在于使数据结构简化。而有些数据必须有具体数值,则此类数据为实质性数据或有意义数据。

account 账号 适于特定用户名和口令使用的一种访问计算机或网络的方式,通常具有一个本地目录、一个电子邮件收信信箱和一组访问特权。

account lockout 账号锁定 账号锁定是连续登录失败后所发生的情况。这可以防范硬性攻击或者人们手工接连尝试口令。大多数操作系统允许在账号被锁定前许可尝试的规定次数(传统的次数是 3)。

account policies 账号策略 包括 Linux 在内的许多操作系统中,可以为每个用

户建立登录和口令规则。例如，用户有效口令有多长？是否允许用户修改它？这些策略就是账号策略。

accountability 可确认性，职能 1. 对各种安全性事件的检查、跟踪和记录，这是业务控制的主要范围。它提供了信息系统安全事件的证明(Proof)和根据(Evidence)。2. 作用在系统上的活动功能。它可使个人及其相关的信息技术产品联系起来，以识别对控制目标的不可预料或不可避免的失误；借助这个功能可以追查自动数据处理系统内行为责任者的性质或状态；可以追查系统各种活动的责任者对其行为负责。

accounting management 记账管理 网络管理功能之一。该功能是商用计算机网络的重要网络管理功能，也常用于非商业化的网络中统计网络用户使用网络资源的情况。

Accounting number 账号 为便于控制而给某项通信安全物资分配的号码。

accreditation 认可，鉴定，审批；身份鉴定 1. 证明一个系统满足事先规定的安全准则的过程。同意授权和批准某个计算机系统或网络在运行环境下处理敏感数据。2. 授权机构颁发的证书，用以证明你的 Web 站点和商业业务是安全的或者适用于安全环境。网络经过严格评估后可以获得该证书。最终结果是认可和同意签署。许多组织都提供这类授权，包括国际计算机安全协会(ICSA)、美国合格公共会计师协会(AICPA)等。3. 在多用户的信息系统中，每个已登记注册的用户可以调用由系统规定的(计算机)资源。为了合法地进入系统，用户把由系统规定的密码口令(password)提交给系统，系统对密码口令加以鉴定，这就是"身份鉴定"。密码口令可以由用户将密钥输入系统，或是用录有密码口令的磁卡输入系统。身份鉴定是信息系统进入子系统的一个组成部分。

accreditation package 核准包 由系统安全计划(SSP)和说明核准决定依据的报告组成的产品。

accrediting authority 认可机构 指定审批机构(DAA)的同义词。

acdountability 可追究性 1.(信息系统中)一种过程，它可使对信息系统活动进行的审计得以追踪到应对这些活动负责的源头。2.(信息安全中)一项原则，它要求委托个人来保护和控制设备、密钥物资及信息，若该设备或信息丢失或误用，即由它向有关机构负责。

ACE Encrypt ACE Encrypt 加密算法 由瑞典 IBM 苏黎世实验室开发的一种新的公钥加密算法。该加密算法已得到欧洲 NESSIE(信号完整性和加密的欧洲新方案)工程的认可。

ACL 访问控制表 见 Access Control List。

ACM (美国)计算机协会 见 Association for Computing Machinery。

ACOPS 自动 CPU 过热保护 ACOPS (Automatic CPU Overheat Prevention System)特指一类计算机主板的一种功能。此类主板在 CPU 插槽的中央有一个温度传感器，当 CPU 散热不佳或散热风扇不转导致 CPU 温度超出安全范围时，系统会通过喇叭发出警告并自动执行降温程序。ACOPS 有自己独立的电路和软件，无需任何驱动程序来启动。

action 操作 一种访问控制表(ACL)许可权属性。参见 access control list。

action agent　响应代理　当控制中心掌握了入侵事件的确切原因和来源后，派出响应代理执行保护和响应的任务。响应代理执行的任务可包括向控制台管理员报警、发出重置连接的数据包、中止非授权访问或者执行反击任务等。

active attack　主动攻击　一种导致非授权状态变化的攻击。主动攻击破坏数据的完整性和有效性，或冒充合法信息来混淆视听、破坏决策。主动攻击一般在被动攻击的基础上进行。攻击可能基于网络或系统的缺陷或后门进行，如利用旧系统的 SENDMAIL 中的一个缺陷，攻击者可以唤起 SHELL。攻击也可能利用管理缺陷或操作员对安全的忽略进行，如通过猜测某人的口令从而进入系统，再利用此人的权限进一步攻击系统的其他用户。

active defend　主动防御　所谓主动防御是指采取技术手段，如入侵检测等，及时地发现网络攻击行为。并及时采取应对措施，如跟踪和反攻击网络攻击者，设置网络陷阱捕捉攻击者，切断网络连接或恢复系统正常工作。

active response　主动响应　入侵检测系统的主动响应就是当一次攻击或入侵被检测到，它自动做出一些动作。主动响应通常分成三类：收集相关信息、改变环境、反击攻击者。

active threat　主动威胁　使系统状态发生非授权改变的威胁。

active wiretapping　主动搭线窃听，篡改信道信息　1. 把未经批准的装置（如计算机终端）连接一个设备（比如一个终端到一条通信通路），通过生成错误信息或控制信号，或者通过改换合法用户的通信方式以获取对该通路中未授权访问的过程。2. 一种在通信信道上进行的破坏活动。破坏活动一般有两类：一是窃听，一是篡改信道信息（也称主动窃听）。

activity　可触发性　计算机病毒一般都有一个触发条件，即在一定的条件下可激活病毒的传染机制使之进行传染。触发条件可以是外界的，也可以是系统内部的，但对病毒本身而言，激发条件都是外部因素。因为一种病毒只是设置一定的激发条件，这个激发条件的判断是病毒自身的功能，而条件则不是病毒自身提供的。一个病毒程序可以按照设计者的要求，在某个点上激活并对系统发起攻击。

AD　管理域　见 Administrative Domain。

Ada　Ada 语言　由美国国防部（DOD）研制的一种高级程序设计语言，并被美国国防部应用于所有的军事程序设计。Ada 基于 Pascal 语言，采用结构化程序设计原则，包括使用能够单独编译的程序模块。Ada 程序可读性强，因而易于维护。Ada 是美国国防部的注册商标。

ADAPSO Guidelines　ADAPSO 指南　数据处理服务组织协会（Association of Data Processing Service Organizations）发出的涉及软件保护方案的准则。

adapter　适配器　插入计算机扩展槽中的一块电路板，为计算机提供扩充功能。它与“卡”是同义词。个人计算机上使用的通用适配器包括提供视频输出的视频适配器、存储器扩充板、内部调制解调器和声卡等。

adaptive-chosen-ciphertext　自适应选定密文　选定密文攻击的一种类型，其中密码分析人员可以动态地选择密文。当密码分析人员能随意使用某个译码

硬件(密码设备)时,他就可以从一个脚本中发动这类攻击,但是他无法从中获取译码密钥。

adaptive-chosen-plaintext 自适应选定明文 选定明文攻击的一种特殊范例,密码分析人员可以动态地选择明文,并根据以前加密的结果改变其选择。

Adaptive Network Security Model (ANSM) 可适应性网络安全模型 ISS公司提出的一种全球网络安全标准。可适应性网络安全模型可以用下面这样的公式概括:安全 = 风险分析 + 执行策略 + 系统实施 + 漏洞监测 + 实时响应。

adaptive routing 自适应路由 设计用来适应当前网络负载的路由,以绕过网络瓶颈点和阻塞区。

add-on security 附加安全 1.为某个运行中的信息系统添加新的硬件、软件或固件保护措施。2.在计算机系统已经交付使用以后,再增加其安全功能的方法。

Add-on security controls 附加安全控制 附件安全控制是事后添加的安全控制,常见于老式的硬件和软件(或者一种安全改进形式和加强老式系统有限安全性能的一种尝试)。

additive system 加乱 按规定的运算方式,将乱数序列与底码序列相结合变成密文的一种密码体制。

address 地址 1.表示 Internet 上一台计算机或现场的一种特殊标识符,它可以是数字 IP 地址(逻辑地址)或文本域名地址(物理地址)。2.一个非常具体的电子邮件地址。

address command 地址命令 一种 UUCP 扩展,它为 UUCP 的基本文件拷贝事务提供额外的路径选择和确认任选项。

Address Mapping Table(AMT) 地址映射表 用来将物理地址转换成逻辑地址的一种表。

address mask 地址掩码 网络地址中标识网络和子网络的部分。

address resolution 地址转换 从物理地址到逻辑地址的转换。在与 Internet 连接的局域网(LAN)中,该过程自动地将每个工作站的 LAN 地址转换为 IP 地址。由于 Internet 和 LAN 处理工作站地址的方式不同,因此需要转换。这种转换由基于地址转换协议(ARP)的程序处理。

Address Resolution Protocol(ARP) 地址转换协议 1.一种把物理地址转换成逻辑地址的 TCP/IP 协议。2.一种 Internet 标准,它为局域网上的工作站提供 IP 地址。

addressing 寻址,编址 网络上识别住处源或消息源的一种方法,不同的网络具有不同的寻址方法。

ADF 访问控制决策单元 ADF 是 Access control decision function 的简称,指实现访问控制的一个判断逻辑或判断函数。

ADMD 公用管理域 ADMD(Administration Management Domain)是由国家所设定的一种管理域,用来与其他国家的电子信箱系统(E-mail)相连接。一个国家可允许有多个 ADMD 同时存在。在其下面可包含专用管理域 PRMD(Private Management Domain),它不能直接与国际上的其他电子信箱系统联网。

Administrative Domain(AD) 管理域 由一个管理员监视的网络部分。

Administrative procedures to guard data integrity, confidentiality and availability 保护数据完整性、机密性和可用性的管理规程 对保护数据的安全措施进行选择和执行以及对与数据保护有关的个人行为进行管理的正式书面管理制度。

administrative security 管理安全 为数据提供适当的保护而制定的管理限制和附加控制。同义词:规程安全 procedural security。

Administrative Terminal System(ATS) 管理终端系统 一种办公自动化系统。它的终端通过双向通信线和计算机相连。在程序控制下,打字员可把文稿打入计算机,并对文稿进行修改和校正。最后,由计算机打印出修改过的稿件。

administrator 管理员 1. 系统管理员(运行网络的人)。2. 为电子邮件论坛或其他 Internet 专题组维护地址和处理杂务的人。

ADP System Security 自动数据处理系统安全 Automatic Data Processing System Security 的简称,指已建立并应用于计算机硬件、软件和数据以便确保组织资产和个人秘密的所有技术防护和管理的规程。

ADPSS 自动数据处理系统安全 见 ADP System Security。

Advanced Encryption Standard(AES) 高级加密标准 美国国家标准与技术研究院(NIST)所开发的一种新的加密标准,用于保证政府信息的安全。1998 年 8 月 20 日,NIST 召开了第一次 AES 候选会议,并公布了 15 个符合基本要求的候选算法,但对它们的安全性未作评估。1999 年 3 月 22 日,NIST 举行了第二次 AES 候选会议,公布了 15 个候选算法的讨论结果,并从中选出了 5 个候选者,它们是 MARS, RC6, Rijndael, SERPENT 和 Twofish。2000 年 10 月 2 日,NIST 公布了最终评选结果,获胜者是 Rijndael 算法。该算法属对称分组密码,支持 128 位的密钥长度。

Advanced Research Projects Agency (ARPA) 远景研究规划局 美国国防部下辖的一个局,现称国防部远景研究规划局(DARPA),它为美国的一些重大计算机技术开发提供主要的资助。20 世纪 60 年代末、70 年代初,ARPA 资助一些大学和研究机构开发了 ARPA 计算机网(Internet 的前身)。另外,它还资助开发了为在全世界普及广域网(WAN)奠定基础的 TCP/IP 协议。

advanced setup options 高级安装选择项 BIOS 安装程序中的一些选择项。用户可以选择 PCI 中断、端口地址和硬盘等安装选择项。错误地设置安装选择项会损坏计算机,因此在修改它们时,一定要小心谨慎。

adversary 对手,敌手 必须拒绝其访问重要信息、技术、系统或子系统的个人、团体组织或政府。

advisory 动向报告 对一个组织的信息系统遭受威胁的重要新动向或发展趋势进行评定。这种评定可包括深入分析对手攻击信息系统的动向、意图、技术或战术。

AEF 访问控制执行单元 AEF 是 Access control enforcement function 的简称,指实现访问控制的一段代码和监听程序。

AES 高级加密标准 见 Advanced En-