中国标准出版社第四编辑室　编

信息安全标准汇编

基础卷

中国标准出版社

信息安全标准汇编

基础卷

中国标准出版社第四编辑室　编

中国标准出版社

北京

图书在版编目（CIP）数据

信息安全标准汇编. 基础卷/中国标准出版社第四编辑室编. —北京：中国标准出版社，2009

ISBN 978-7-5066-5239-1

Ⅰ.信… Ⅱ.中… Ⅲ.信息系统-安全技术-国家标准-汇编-中国 Ⅳ.TP309-65

中国版本图书馆 CIP 数据核字（2009）第 044290 号

中国标准出版社出版发行
北京复兴门外三里河北街 16 号
邮政编码：100045

网址 www.spc.net.cn
电话：68523946 68517548
中国标准出版社秦皇岛印刷厂印刷
各地新华书店经销

*

开本 880×1230 1/16 印张 37.75 字数 1 152 千字
2009 年 4 月第一版 2009 年 4 月第一次印刷

*

定价 194.00 元

出 版 说 明

在信息化社会，信息技术飞速发展，随之而来的信息技术的安全问题日益突出，它关系到信息系统的正常运行和健康发展，影响到信息化社会的各个方面，不容忽视。国家标准化管理委员会已制定和发布了一系列信息安全国家标准，为我国信息系统的安全提供了技术支持，为信息安全的监督和管理提供了依据和指导。

为满足广大信息技术人员的需求，方便学习和查阅，我们将信息安全国家标准按照信息安全标准体系收集、分类、汇编成卷，共分为以下5卷：

——基础卷

——信息安全管理卷

——信息安全测评卷

——技术与机制卷

——密码技术卷

其中信息安全测评卷、技术与机制卷根据需要又分为若干分册。

随着信息安全标准体系的完善和标准制修订情况的变化，本套汇编将陆续分卷分册出版。

本卷为基础卷，共收入截至2009年2月发布的有关信息安全术语、体系结构、模型、框架标准17项。

编　　者

2009年2月

目　　录

前　言

本标准等同采用国际标准ISO/IEC 2382-8:1998《信息技术　词汇　第8部分:安全》。

本标准是对国家标准GB/T 5271.8—1993的修订,根据信息技术的发展和变化,本标准着重于计算机安全方面的术语词汇,标题由原来的《数据处理词汇　08部分　控制、完整性和安全性》改为《信息技术　词汇　第8部分　安全》,内容上只保留原标准有关安全方面的词汇18个词条,另外新增加了170个信息技术安全术语词条。

制定信息技术词汇标准的目的是为了方便信息技术的国内外交流。它给出了与信息处理领域相关的概念的术语及其定义,并明确了各术语词条之间的关系。本标准定义了有关密码术、信息分类与访问控制、数据与信息恢复和安全违规等概念。

GB/T 5271系列标准由30多个部分组成,都在总标题《信息技术　词汇》之下。本标准是GB/T 5271系列标准的第8部分。

本标准由中华人民共和国信息产业部提出。

本标准自实施之日起,代替和废止国家标准GB/T 5271.8—1993。

本标准由中国电子技术标准化研究所归口。

本标准起草单位:中国电子技术标准化研究所。

本标准主要起草人:陈莹、王保艾。

ISO/IEC 前言

ISO(国际标准化组织)和 IEC(国际电工委员会)是世界性的标准化专门机构。国家成员体(它们都是 ISO 或 IEC 的成员国)通过国际组织建立的各个技术委员会参与制定针对特定技术领域的国际标准。ISO 和 IEC 的各技术委员会在共同感兴趣的领域内进行合作。与 ISO 和 IEC 有联系的其他官方和非官方国际组织也可参与国际标准的制定工作。

对于信息技术,ISO 和 IEC 建立了一个联合技术委员会,即 ISO/IEC JTC1。由联合技术委员会提出的国际标准草案需分发给各国家成员体进行表决。发布一项国际标准,至少需要 75%的参与表决的国家成员体投票赞成。

国际标准 ISO/IEC 2382-8 是由 ISO/IEC JTC1 信息技术联合技术的 SC1 词汇分委员会制定的。

ISO/IEC 2382 由 30 多个部分组成,都在总标题“信息技术　词汇”之下。

中华人民共和国国家标准

信息技术　词汇
第8部分：安全

GB/T 5271.8—2001
idt ISO/IEC 2382-8:1998

代替 GB/T 5271.8—1993

Information technology—Vocabulary—Part 8:Security

1　概述

1.1　范围

为便于信息和数据安全保护方面的国内外交流，特制定本标准。本标准给出了与信息技术领域相关的概念的术语和定义，并明确了这些条目之间的关系。

为方便本标准翻译成其他少数民族语言，本标准各条词汇的定义中尽可能避免使用语言中偏特的词语。

本标准定义了有关密码术、信息分类与信息访问控制、数据与信息的恢复和安全违规等数据与信息安全保护方面的概念。

1.2　引用标准

下列标准所包含的条文，通过在本标准中引用而构成为本标准的条文。本标准出版时，所示版本均为有效。所有标准都会被修订，使用本标准的各方应探讨使用下列标准最新版本的可能性。

GB/T 2659—2000　世界各国和地区名称代码(eqv ISO 3166-1:1997)

GB/T 9387.2—1995　信息处理系统　开放系统互连　基本参考模型　第2部分：安全体系结构(idt ISO 7498-2:1989)

GB/T 15237.1—2000　术语工作　词汇　第1部分　理论与应用(eqv ISO 1087-1:2000)

1.3　遵循的原则和规则

1.3.1　词条的定义

第2章包括许多词条。每个词条由几项必需的要素组成，包括索引号、一个术语或几个同义术语和定义一个概念的短语。另外，一个词条可包括举例、注解或便于理解概念的解释。

有时同一个术语可由不同的词条来定义，或一个词条可包括两个或两个以上的概念，说明分别见1.3.5和1.3.8。

本标准使用其他的术语，例如词汇、概念、术语和定义，其意义在GB/T 15237.1中有定义。

1.3.2　词条的组成

每个词条包括1.3.1中规定的必需的要素，如果需要，可增加一些要素。词条按以下的顺序包括如下要素：

a）索引号；

b）术语在语言中的概念若没有首选术语表示，用五个点的符号表示(.....)；在一个术语中，一行点用来表示每个特定事例中被选的一个词；

c）首选术语(根据GB/T 2659规则标明)；

d）术语的缩略语；

中华人民共和国国家质量监督检验检疫总局2001-07-16批准　　2002-03-01实施

e) 许可的同义术语；

f) 定义的正文(见 1.3.4)；

g) 以“例子”开头的一个或几个例子；

h) 以“注”开头的概念应用领域标明特殊事例的一个或几个注解；

i) 词条共用的图片、图示或表格。

1.3.3 词条的分类

本系列标准的每部分被分配两个数字组成的序列号，并以表示“基本术语”的 01 开始。

词条按组分类，每组被分配一个四个数字组成的序列号；前两个数字表示该组在本标准中所处的部分。

每个词条被分配一个六个数字组成的索引号；前四个数字表示该词条所在的标准部分和组。

1.3.4 术语的选择和定义的用语

选择术语和定义用语尽可能按照已规定的用法。当出现矛盾时，采用大多数同意的方法。

1.3.5 多义术语

在一种工作语言中，如果一个给定的术语有几个意义，每个意义则给定一个单独的词条以便于翻译成其他的语言。

1.3.6 缩略语

如 1.3.2 中所指，当前使用的缩略语被指定给一些术语。这些缩略语不用于定义、例子或注解的文字中。

1.3.7 圆括弧的用法

在一些术语中，按黑体字印刷的一个词或几个词置于括弧中。这些词是完整术语的一部分。

当在技术文章中使用缩略术语不影响上下文的意思时，这些词可被省略。在 GB/T 5271 的定义、例子或注解的正文中，这些术语按完整形式使用。

在一些词条中，术语后面跟着普通字体的放在括弧中的文字。这些词不是术语的某部分，而是指明使用该术语的有关信息，如它的特殊的应用范围，或它的语法形式。

1.3.8 方括弧的用法

如果几个紧密相关的术语的定义只是几个文字的区别，这些术语及其定义归为一个词条。为表示不同的意思的替换文字按在术语和在定义中的相同的次序放在方括弧中。为避免被替换词的不明确性，按上述规则放在括弧前面的最后一个词可放在方括弧里面，并且每变化一次则重复一次。

1.3.9 定义中黑体术语的用法和星号的用法

术语在定义、例子或注解中用黑体字印刷时，则表示该术语已在本词汇的其他词条中定义过。但是，只有当这些术语首次出现在每一个词条中时，该术语才印成黑体字的形式。

黑体也用于一个术语的其他语法形式，如名词复数和动词的分词形式。

定义在 GB/T 5271 中所有以黑体出现的术语的基本形式列在本部分后面的索引中(见 1.3.10)。

当在不同的词条中引用的两个黑体术语一个紧接着另一个，用星号将二者分隔开(或仅用标点分隔)。

以一般字体出现的词或术语，按一般词典中或权威性技术词汇的释义理解。

1.3.10 索引表的编制

对于使用的每一种语言，在每部分的结尾提供字母索引。索引包括该部分定义的所有术语。

多词术语按字母顺序出现在每个关键字后。

2 术语和定义

08 安全

08.01 一般概念

08.01.01 **计算机安全 computer security**
COMPUSEC(缩略语) **COMPUSEC**(abbreviation)
通常采取适当行动保护**数据**和**资源**,使它们免受偶然或恶意的动作。
注:这里偶然或恶意的动作可指未经授权的修改、破坏、访问、**泄露**或获取。

08.01.02 **管理性安全 administrative security**
过程安全 procedural security
用于**计算机安全**的管理措施。
注:这里的措施可以是可操作的**可核查性**过程、调查安全**违规**的过程和审查**审计跟踪**的过程。

08.01.03 **通信安全 communication security**
COMSEC(缩略语) **COMSEC**(abbreviation)
适用于**数据通信**的**计算机安全**。

08.01.04 **数据安全 data security**
适用于**数据**的**计算机安全**。

08.01.05 **安全审计 security audit**
对**数据处理系统**记录与活动的独立的审查和检查,以测试系统控制的充分程度,确保符合已建立的**安全策略**和操作过程,检测出安全**违规**,并对在控制、安全策略和过程中指示的变化提出建议。

08.01.06 **安全策略;安全政策 security policy**
为保障**计算机安全**所采取的行动计划或方针。

08.01.07 **数据完整性 data integrity**
数据所具有的特性,即无论数据形式作何变化,数据的准确性和一致性均保持不变。

08.01.08 **文件保护 file protection**
为了防止对**文件**未经授权地访问、修改或删除,而采取适当的管理、技术或物理手段。

08.01.09 **保密性;机密性 confidentiality**
数据所具有的特性,即表示数据所达到的未提供或未泄露给未授权的个人、过程或其他**实体**的程度。

08.01.10 **可核查性 accountability**
一种特性,即能保证某个**实体**的行动能唯一地追溯到该实体。

08.01.11 **鉴别 authentication**
验证**实体**所声称的身份的动作。

08.01.12 **消息鉴别 message authentication**
验证*消息是由声明的**始发者**发给**预期的接收者**,并且验证该消息在转移中未被更改。

08.01.13 **鉴别信息 authentication information**
用来确立**实体**所声称身份的有效性的**信息**。

08.01.14 **凭证 credentials**
为确立**实体**所声称的身份而**传送**的**数据**。

08.01.15 **鉴别交换 authentication exchange**
借助**信息交换**手段以保证**实体**身份的一种机制。

08.01.16 **授权 authorization**
给予权利,包括**访问权**的授予。

08.01.17 **可用性**(用于计算机安全) **availability** (in computer security)
数据或**资源**的特性,被授权**实体**按要求能访问和使用数据或资源。

08.01.18 **认证**(用于计算机安全) **certification** (in computer security)

第三方作出保证**数据处理系统**的全部或部分符合安全要求的过程。

08.01.19 **安全许可** **security clearance;clearance**

许可个人在某一特定的**安全级别**或低于该级别**访问*数据**或**信息**。

08.01.20 **安全级别** **security level**

分层的**安全等级**与表示**对象**的敏感度或个人的**安全许可**的**安全种类**的组合。

08.01.21 **封闭的安全环境** **closed-security environment**

一种环境，在该环境下特别着重(通过**授权**、**安全许可**、配置控制等形式)对**数据**和**资源**的保护，使之免受偶然的或恶性的动作。

08.01.22 **开放的安全环境** **open-security environment**

一种环境，通过普通的操作过程即可获得对**数据**及**资源**的保护，使之免受偶然的或恶性的动作。

08.01.23 **隐私权** **privacy**

防止因不正当或非法收集和使用个人**数据**而对个人的私生活或私事进行侵犯。

08.01.24 **风险分析** **risk analysis**

风险评估 **risk assessment**

一种系统的方法，标识出**数据处理系统**的资产、对这些资产的**威胁**以及该系统对这些威胁的**脆弱性**。

08.01.25 **风险接受** **risk acceptance**

一种管理性的决定，通常根据技术或成本因素，决定接受某一程度的**风险**。

08.01.26 **敏感性** **sensitivity**

信息拥有者分配给**信息**的一种重要程度的度量，以标出该信息的保护需求。

08.01.27 **系统完整性** **system integrity**

在防止非授权用户修改或使用资源和防止授权用户不正确地修改或使用**资源**的情况下，**数据处理系统**能履行其操作目的的品质。

08.01.28 **威胁分析** **threat analysis**

对可能损害**数据处理系统**的动作和事件所做的检查。

08.01.29 **可信计算机系统** **trusted computer system**

提供充分的**计算机安全**的**数据处理系统**，它允许具有不同**访问权**的用户**并发访问*数据**，以及访问具有不同**安全等级**和**安全种类**的数据。

08.01.30 **主体**(用于计算机安全) **subject** (in computer security)

能访问**客体**的主动**实体**。

例：涉及**程序*执行**的**过程**。

注：主体可使**信息**在客体之间流动，或者可以改变**数据处理系统**的状态。

08.01.31 **客体**(用于计算机安全) **object** (in computer security)

一种**实体**，对该实体的访问是受控的。

例：**文件**、**程序**、**主存**区域；收集和维护的有关个人的**数据**。

08.02 信息分类

08.02.01 **安全分类；安全等级** **security classification**

决定防止**数据**或**信息**需求的访问的某种程度的保护，同时对该保护程度给以命名。

例："绝密"、"机密"、"秘密"。

08.02.02 **敏感信息** **sensitive information**

由权威机构确定的必须受保护的**信息**，因为该信息的**泄露**、修改、破坏或**丢失**都会对人或事产生可预知的损害。

08.02.03 **安全种类 security category**

一种对**敏感信息**非层次的分组，此方法比仅用分层次的**安全等级**能更精细地控制对**数据**的访问。

08.02.04 **分隔 compartmentalization**

将**数据**划分成有独立安全控制的隔离块，以便减少**风险**。

例：将与主项目相关的数据分成与各子项目相对应的块，每个块有其自己的安全保护，这样能减小**暴露**整个项目的可能性。

08.02.05 **多级设备 multilevel device**

一种**功能单元**，它能同时处理两个或多个**安全级别**的**数据**而不会危及**计算机安全**。

08.02.06 **单级设备 single-level device**

一种**功能单元**，它在某一时刻只能处理一个**安全级别**的**数据**。

08.03 密码技术

08.03.01 **密码学；密码术 cryptography**

一种学科，包含数据变换的原则、手段和方法，以便隐藏**数据**的语义内容，防止未经授权的使用或未检测到的修改。

08.03.02 **加密 encryption；encipherment**

数据的密码变换。

注

1 加密的结果是**密文**。

2 相反的过程称为**解密**。

3 也见**公钥密码**、**对称密码**和**不可逆加密**。

08.03.03 **不可逆加密 irreversible encryption；irreversible encipherment**

单向加密 one-way encryption

一种**加密**，它只产生**密文**，而不能将密文再生为原始**数据**。

注：不可逆加密用于**鉴别**。例如，**口令**可被不可逆地加密，产生的密文被**存储**。后来出示的口令将同样被不可逆地加密，然后将两**串**密文进行比较。如果他们是相同的，则后来出示的口令是正确的。

08.03.04 **解密 decryption；decipherment**

从**密文**中获取对应的原始**数据**的过程。

注：可将密文再次加密，这种情况下单次解密不会产生原始**明文**。

08.03.05 **密码系统 cryptographic system；ciphersystem；cryptosystem**

一起用来提供**加密**或**解密**手段的文件、部件、设备及相关的技术。

08.03.06 **密码分析 cryptanalysis**

分析**密码系统**、它的**输入**或**输出**或两者，以导出**敏感信息**，例如**明文**。

08.03.07 **明文 plaintext；cleartext**

无需利用密码技术即可得出语义内容的**数据**。

08.03.08 **密文 ciphertext**

利用**加密**产生的**数据**，若不使用密码技术，则得不到其语义内容。

08.03.09 **密钥**（用于计算机安全） **key** (in computer security)

控制**加密**或**解密**操作的**位串**。

08.03.10 **私有密钥；私钥 private key**

为拥有者专用于**解密**的**密钥**。

08.03.11 **公开密钥；公钥 public key**

一种**密钥**，任意**实体**都可用它与相对应的**私钥**拥有者进行加密通信。

08.03.12 **公钥密码术** **public-key cryptography**
非对称密码术 **asymmetric cryptography**
用**公开密钥**和对应的**私有密钥**进行**加密**和**解密**的**密码术**。
注：如果公钥用于加密，则对应的私钥必须用于解密，反之亦然。

08.03.13 **对称密码术** **symmetric cryptography**
同一**密钥**既用于**加密**也用于**解密**的**密码术**。

08.03.14 **秘密密钥** **secret key**
由有限数目的通信者用来**加密**和**解密**的**密钥**。

08.03.15 **换位** **transposition**
一种**加密**方法，即按照某一方案重新排列**位**或**字符**。
注：最后所得的**密文**称为换位密码。

08.03.16 **代入** **substitution**
一种**加密**方法，即用其他的**位串**或**字符串**代替某些位串或字符串。
注：所得**密文**称为替代密码。

08.04 访问控制

08.04.01 **访问控制** **access control**
一种保证手段，即**数据处理系统**的**资源**只能由被授权**实体**按授权方式进行**访问**。

08.04.02 **访问控制(列)表** **access control list**
访问(列)表 **access list**
由拥有**访问权利**的**实体**组成的列表，这些实体被授权**访问**某一**资源**。

08.04.03 **访问类别** **access category**
根据**实体**被授权使用的**资源**，对实体分配的类别。

08.04.04 **访问级别** **access level**
实体对受保护的**资源**进行**访问**所要求的权限级别。
例：在某个**安全级别**上授权访问**数据**或**信息**。

08.04.05 **访问权** **access right**
允许**主体**为某一类型的**操作*访问**某一**客体**。
例：允许某**过程**对**文件**有**读**权，但无**写**权。

08.04.06 **访问许可** **access permission**
主体针对某一**客体**的所有的**访问权**。

08.04.07 **访问期** **access period**
规定**访问权**的有效期。

08.04.08 **访问类别**(用于计算机安全) **access type** (in computer security)
由**访问权**所规定的**操作**类型。
例：**读**、**写**、**执行**、添加、修改、删除与创建。

08.04.09 **权证**(用于计算机安全) **ticket** (in computer security)
访问权拥有者对某**主体**所拥有的一个或多个访问权的表示形式。
注：标签代表**访问许可**。

08.04.10 **资质**(用于计算机安全) **capability** (in computer security)
标识一个**客体**、或一类客体、或这些客体的一组授权**访问类型**的表示形式。
注：资质能以**权证**形式来实现。

08.04.11 **资质(列)表** **capability list**
与**主体**相关的列表，它标识出该主体对所有**客体**的所有**访问类型**。

例：有关某一过程的列表，标识出该过程对所有**文件**及其他受保护**资源**的所有访问类型。

08.04.12 **身份鉴别 identity authentication；**
身份确认 identity validation
使**数据处理系统**能识别出**实体**的测试实施过程。
例：检验一个**口令**或**身份权标**。

08.04.13 **身份权标 identity token**
用于**身份鉴别**的物件。
例：智能卡、金属钥匙。

08.04.14 **口令 password**
用作**鉴别信息**的**字符串**。

08.04.15 **最小特权 minimum privilege**
主体的**访问权**限制到最低限度，即仅执行授权任务所必需的那些权利。

08.04.16 **需知 need-to-know**
数据的预期**接收者**对数据所表示的**敏感信息**要求了解、**访问**、或者拥有的合法要求。

08.04.17 **逻辑访问控制 logical access control**
使用与**数据**或**信息**相关的机制来提供**访问控制**。
例：**口令**的使用。

08.04.18 **物理访问控制 physical access control**
使用物理机制提供**访问控制**。
例：将**计算机**放在上锁的房间内。

08.04.19 **受控访问系统 controlled access system**
CAS(缩略语) **CAS**(abbreviation)
使**物理访问控制**达到**自动化**的方法。
例：使用磁条证、智能卡、**生物测定**阅读器等。

08.04.20 **读访问 read access**
一种**访问权**，它允许**读***数据。

08.04.21 **写访问 write access**
一种**访问权**，它允许**写***数据。
注：写访问可允许添加、修改、删除或创建数据。

08.04.22 **用户标识 user ID；user identification**
一种**字符串**或**模式**，**数据处理系统**用它来标识用户。

08.04.23 **用户简介**(1) **user profile** (1)
对用户的描述，一般用于**访问控制**。
注：用户简介包括这样一些**数据**，如**用户标识**、用户名、**口令**、**访问权**及其他属性。

08.04.24 **用户简况**(2) **user profile** (2)
用户的活动**模式**，可以用它来检测出活动中的变化。

08.05 安全违规

08.05.01 **计算机滥用 computer abuse**
影响或涉及**数据处理系统**的**计算机安全**的蓄意的或无意的未经授权的活动。

08.05.02 **计算机犯罪 computer crime**
借助或直接介入**数据处理系统**或**计算机网络**而构成的犯罪。
注：本定义是对 GB/T 5271.1—2000 中本条定义的改进。

08.05.03 **计算机诈骗 computer fraud**

借助或直接介入**数据处理系统**或**计算机网络**而构成的诈骗。

08.05.04 **威胁 threat**

一种潜在的**计算机安全**违规。

注：见图1。

08.05.05 **主动威胁 active threat**

未经授权对**数据处理系统**状态进行蓄意的改变而造成的**威胁**。

例：这种威胁将造成**消息**的修改、伪造消息的插入、服务**假冒**或**拒绝服务**。

08.05.06 **被动威胁 passive threat**

泄露*信息，但不改变**数据处理系统**状态所造成的**威胁**。

例：这种威胁将造成因截获所**传送**的**数据**而导致**敏感信息**的透露。

08.05.07 **纰漏**(用于计算机安全) **flaw** (in computer security);**loophole**

委托出错、遗漏或疏忽，从而使保护机制被避开或失去作用。

08.05.08 **脆弱性 vulnerability**

数据处理系统中的弱点或**纰漏**。

注

1 如果脆弱性与**威胁**对应，则存在**风险**。

2 见图1。

08.05.09 **风险 risk**

特定的**威胁**利用**数据处理系统**中特定的**脆弱性**的可能性。

注：见图1。

08.05.10 **拒绝服务 denial of service**

资源的授权访问受阻或关键时刻的**操作**的延误。

08.05.11 **泄密 compromise**

违反**计算机安全**，从而使**程序**或**数据**被未经授权的**实体**修改、破坏或使用。

注：见图1。

08.05.12 **损失 loss**

对因**泄密**所造成的损害或丧失的量化的度量。

注：见图1。

08.05.13 **暴露 exposure**

特定的**攻击利用数据处理系统**特定的**脆弱性**的可能性。

注：见图1。

08.05.14 **泄密辐射 compromising emanation**

无意辐射的**信号**，如果被窃听或被分析，这些信号就会透露正被处理或**发送**的**敏感信息**。

08.05.15 **泄露 disclosure**

计算机安全的违规，使**数据**被未经授权的**实体**使用。

08.05.16 **侵入 penetration**

对**数据处理系统**进行未经授权的访问。

注：见图1。

08.05.17 **违规 breach**

在检测或未经检测的情况下，**计算机安全**的某一部分被避开或失去作用，它可能产生对**数据处理系统**的**侵入**。

注：见图1。

08.05.18 **网络迂回 network weaving**

一种**侵入**技术，即用不同的通信**网络**来访问**数据处理系统**，以避开检测和回溯。

08.05.19 **攻击 attack**

违反**计算机安全**的企图。

例：**恶性逻辑**、**窃听**等。

注：见图1。

08.05.20 **分析攻击 analytical attack**

密码分析攻击 cryptanalytical attack

运用分析方法解开**代码**或找到**密钥**的企图。

例：**模式**的统计分析；搜索**加密***算法中的**纰漏**。

注：与**穷举攻击**相对。

08.05.21 **唯密文攻击 ciphertext-only attack**

一种**分析攻击**，其中密码分析者只占有**密文**。

08.05.22 **已知明文攻击 known-plaintext attack**

一种**分析攻击**，其中密码分析者占有相当数量互相对应的**明文**和**密文**。

08.05.23 **选择明文攻击 chosen-plaintext attack**

一种**分析攻击**，其中密码分析者能选定无限的**明文***消息并检查相对应的**密文**。

08.05.24 **穷举攻击 exhaustive attack；brute-force attack**

通过尝试**口令**或**密钥**可能有的值，违反**计算机安全**的企图。

注：与**分析攻击**相对。

08.05.25 **窃取 eavesdrop**

未经授权地截取承载**信息**的辐射信号。

08.05.26 **线路窃听 wiretapping**

暗中访问**数据电路**的某部分，以获得、修改或插入**数据**。

08.05.27 **主动线路窃听 active wiretapping**

一种**线路窃听**，其目的是修改或插入**数据**。

08.05.28 **被动线路窃听 passive wiretapping**

一种**线路窃听**，其目的只局限于获取**数据**。

08.05.29 **冒充 masquerade**

一个实体假装成另一个**实体**，以便获得未经授权的访问权。

08.05.30 **暗入 piggyback entry**

通过授权用户的合法连接对**数据处理系统**进行未经授权的访问。

08.05.31 **跟入 to tailgate**

紧跟授权人通过受控门获得未经授权的物理访问。

08.05.32 **捡残 to scavenge**

未经**授权**，通过**残余数据**进行搜索，以获得**敏感信息**。

08.05.33 **迷惑 to spoof**

为欺骗用户、观察者(如监听者)或**资源**而采取的行动。

08.05.34 **放弃连接 aborted connection**

不遵循已建立规程而造成的连接断开。

注：放弃连接可使其他**实体**获得未经授权的访问。

08.05.35 **故障访问 failure access**

由于**硬件**或**软件***故障，造成对**数据处理系统**的**数据**未经授权且通常是不经意的访问。

08.05.36 **线路间进入 between-the-lines entry**

未授权用户通过**主动线路窃听**获得对连在合法用户**资源**上的某临时被动**传输信道**的访问

权。

08.05.37 **陷门** **trapdoor**

通常为测试或查找故障而设置的一种隐藏的**软件**或**硬件**机制，它能避开**计算机安全**。

08.05.38 **维护陷门** **maintenance hook**

软件中的**陷门**，它有助于**维护**和开发某些附加功能，而且它能在非常规时间点或无需常规检查的情况下进入**程序**。

08.05.39 **聚合** **aggregation**

通过收集较低**敏感性***信息并使之相互关联而采集**敏感信息**。

08.05.40 **链接**(用于计算机安全) **linkage** (in computer security)

聚接 fusion

有目的地将来自两个不同的**数据处理系统**的**数据**或**信息**组合起来，以导出受保护的信息。

08.05.41 **通信流量分析** **traffic analysis**

通过观察通信流量而推断**信息**。

例：对通信流量的存在、不存在、数量、方向和频次的分析。

08.05.42 **数据损坏** **data corruption**

偶然或故意违反**数据完整性**。

08.05.43 **泛流** **flooding**

因偶然或故意插入大量的**数据**而导致**服务拒绝**。

08.05.44 **混杂** **contamination**

将一个**安全等级**或**安全种类**的**数据**引入到较低安全等级或不同安全种类的数据中。

08.05.45 **隐蔽信道** **covert channel**

可用来按照违反**安全策略**的方式**传送***数据的**传输信道**。

08.05.46 **恶性逻辑** **malicious logic**

在**硬件**、**固件**或**软件**中所实施的**程序**，其目的是执行未经授权的或有害的行动。

例：**逻辑炸弹**、**特洛伊木马**、**病毒**、**蠕虫**等。

08.05.47 **病毒** **virus**

一种**程序**，即通过修改其他程序，使其他程序包含一个自身可能已发生变化的原程序副本，从而完成传播自身程序，当调用受传染的程序，该程序即被**执行**。

注：病毒经常造成某种损失或困扰，并可以被某一事件(诸如出现的某一预定日期)触发。

08.05.48 **蠕虫** **worm**

一种独立**程序**，它可通过**数据处理系统**或**计算机网络**传播自身。

注：蠕虫经常被设计用来占满可用**资源**，如**存储**空间或处理时间。

08.05.49 **特洛伊木马** **Trojan horse**

一种表面无害的**程序**，它包含**恶性逻辑程序**，导致未授权地收集、伪造或破坏**数据**。

08.05.50 **细菌** **bacterium**

链式信件 **chain letter**

一种**程序**，它通过**电子邮件**将自己传播给每一个**接收方**的**分发列表**中的每个人。

08.05.51 **逻辑炸弹** **logic bomb**

一种**恶性逻辑程序**，当被某个特定的系统条件触发时，造成对**数据处理系统**的损害。

08.05.52 **定时炸弹** **time bomb**

在预定时间被激活的**逻辑炸弹**。

08.06 敏感信息的保护

08.06.01 **验证** **verification**