全国信息技术人才培养工程指定培训教材
信息安全理论与实用技术丛书

信息安全实用技术

信息产业部电子教育中心　组编
戴宗坤　主编

XINXI ANQUAN SHIYONG JISHU

重庆大学出版社

全国信息技术人才培养工程指定培训教材

信息安全理论与实用技术丛书

信息安全实用技术

信息产业部电子教育中心摇组编

戴宗坤摇摇摇摇摇　　主编

罗万伯摇方摇勇摇周安民
欧晓聪摇何其超摇戴宗坤　摇编著

重庆大学出版社

前　言

摇摇短短几年时间，信息安全问题已经渗透到社会各个领域，引起人们的深切关注。信息安全问题不是凭空出现的，它是信息化技术高速发展、伴随信息网络化和社会信息化发展进程与生俱来的产物。一般认为，信息安全问题的源头是信息系统及其组件在客观上存在脆弱性和漏洞，在主观上存在利用这些脆弱性和漏洞来达到某种目的或获得某种利益的系统内外部的威胁。这些问题其所以引起全社会的如此重视，是因为国际互联网络技术出现并大规模普及应用后，社会各领域从上到下都感到了问题的严重性。

长期以来，人们知道如何规范自己的行为和自我保护，是因为有成熟的法律体系保障，而且从小就受到学校、家庭和社会的系统安全教育，加之整个社会具有维护传统社会秩序的强大的道德和文化氛围，使得人们有明确的是非判断能力和行为的控制能力，因而具有强烈的安全意识。但当信息化渗透到社会各个领域时，由于信息化进程的高速发展，人们来不及对信息化社会的安全问题——信息系统自身的脆弱性和漏洞，以及由此带来的威胁进行认识或根本不认识，人们没有从法律体系、从道德和文化素质，以及信息安全意识上做好适应社会信息化的心理和技术准备。针对信息化进程中这一带普遍性的问题，近年来我国一方面加强对信息安全有关的法律、法规建设，发展信息安全产业；另一方面从教育和培训做起，采取措施加快信息安全学科建设和人才培养，加强信息安全技术和技能培训，强调全面培养和提高全民族的信息安全道德素质和信息安全意识。

摇摇员怨愿年以来,四川大学信息安全研究所在信息安全学科建设和多层次学历教育上进行了系统地探索和研究,在多年教学和科研成果基础上编辑出版了用于本科和硕士研究生的教材和参考书 ;圆园园缘年开始,与国家信息安全产业成果化 (四川) 基地联合进行信息安全非学历教育和技能技巧的培训,为适应日益增长的培训和教育市场,我们在本科和研究生教材基础上,结合在职继续教育的经验和特点,编写了第一批共 猿本培训教材 (即《信息安全应用基础》,《信息安全实用技术》和《信息安全法律规范及管理》),作为重庆大学出版社《信息安全理论与实用技术系列丛书》的开篇出版,以起抛砖引玉之作用,并为我们在实际培训中采用。

本书共 怨章,第 员章主要对人和实体与信息系统交互的第一安全要素——身份鉴别的原理、方法进行了系统介绍,并对与鉴别有关的 运[illegible]系统和用于建立网络信任体系的 孕[illegible]进行了介绍 ;第 圆章系统地对防火墙技术原理、配置方法和拓扑结构进行了分类介绍,并附实例帮助阅读 ;第 猿章对入侵检测的技术原理、方法以及入侵检测设备和系统的应用做了较为详细的介绍 ;第 源章对 灾[illegible]和网络安全及三者的关系进行了系统研究,特别详解了如何使用灾[illegible]技术在公共网络上构建安全网络平台的原理、方法和工程实现问题,同时对广泛使用的[illegible]技术原理和实现方法进行了详解 ;第 缘章介绍了 [illegible]应用安全 ;第 远章对于在网络安全管理中起重要作用的审计与报警技术的系统知识进行了介绍 ;第 苑章对病毒和恶意代码的技术原理,以及在网络信息系统中如何建立病毒防范体系进行了系统介绍 ;第 愿章剖析了当今名声不好的黑客现象及其沿革,对主要的黑客技术进行了分析,并对如何利用黑客技术为网络安全和国家利益服务进行了探讨 ;第 怨章根据我们的研究成果和经验,对网络信息系统的安全解决方案给出了可供实际裁剪的方法和案例。全书采用理论与工程实际相结合的方法,既有理论依据,又有工程实现方法,相信读者会从中得到自己所需要的东西。

本书第 员章和第 圆章由方勇主笔 ;第 猿章、第 缘章和第 远章由罗万伯主笔,李焕洲协助 ;第 源章由戴宗坤主笔,陈麟协助 ;第 苑章由何其超主笔 ;第 愿章由欧晓聪主笔 ;第 怨章由周安民主笔。全书由戴宗坤主审,罗万伯协助。杨忠、刘军、徐自力等在资料整理等方面参与了工作。作者们在此对为本书出版提供了帮助的所有人,特别是重庆大学出版社的同志们表示衷心的感谢!

本书可作为信息安全专业技术培训教材,亦可作为信息安全和计算机应用本专科教材,并对从事信息安全管理、信息系统管理以及信息安全咨询服务的专业技术人员具有重要使用价值。

由于作者水平和时间限制,书中定有需要商榷甚至错误之处,恳请读者不吝赐教。

编摇者

[illegible]年 愿月 员源日于成都四川大学

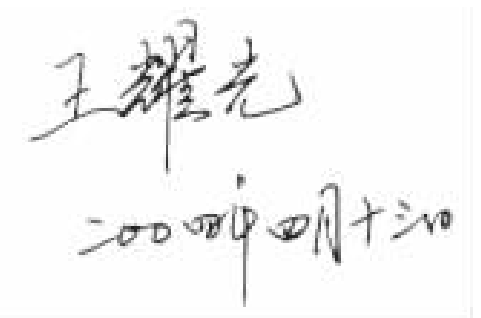
丛书序

摇摇当今世界，随着信息技术在经济社会各领域不断深化的应用，信息技术对生产力以至于人类文明发展的巨大作用越来越明显。党的“十六大”提出要“坚持以信息化带动工业化，以工业化促进信息化”，“优先发展信息产业，在经济和社会领域广泛应用信息技术”。明确了我国经济发展的道路，赋予了信息产业新的历史使命。近年来，日新月异的信息技术呈现出新的发展趋势，各类信息技术加快了相互融合和渗透的步伐，信息技术与其他技术的结合更加紧密，信息技术应用的深度、广度和专业化程度不断提高。

我国的信息产业作为国民经济的支柱产业正面临着有利的国际、国内形势，电子信息产业的规模总量已进入世界大国行列。但是我们也清楚地认识到，与国际先进水平相比，我们在产业结构、核心技术、管理水平、综合效益、普及程度等方面，还存在较大差距，缺乏创新能力与核心竞争力，“大”而不强。国际国内形势的发展，要求信息产业不仅要做大，而且要做强，要从制造大国向制造强国转变，这是信息产业今后的重点工作。要实现这一转变，人才是基础。机遇难得，人才更难得，要抓住本世纪头二十年的重要战略机遇期，加快信息产业发展，关键在于培养和使用好人才资源。《中共中央、国务院关于进一步加强人才工作的决定》指出，人才问题是关系党和国家事业发展的关键问题，人才资源已成为最重要的战略资源，人才在综合国力竞争中越来越具有决定性意义。

为抓住机遇，迎接挑战，实施人才强业战略，信息产业部启动了“全国信息技术人才培养工程”。该项工程旨在通过政府政策引导，充分发挥全行业和全社会教育培训资源的作用，建立规范的信息技术教育培训体系、科学的培训课程体系、严谨的信息技术人才评测服务体系，培养造就大批行业急需的、结构合理的高素质信息技术应用型人才，以促进信息产业持续快速协调健康发展。

摇摇由各方专家依据信息产业对技术人才素质与能力的需求,在充分吸取国内外先进信息技术培训课程优点的基础上,信息产业部电子教育中心精心组织编写了信息技术系列培训教材。这些教材注重提升信息技术人才分析问题和解决问题的能力,对各层次信息技术人才的培养工作具有现实的指导意义。我谨向参与本系列教材规划、组织、编写同志们致以诚挚的感谢,并希望该系列教材在全国信息技术人才培养工作中发挥有益的作用。



圆

全国信息技术人才培养工程教材
编 委 会

目　录

员摇身份鉴别技术 …… 员

摇员援员摇身份鉴别 …… 圆

摇摇员援员援员摇鉴别的基本概念 …… 圆

员援员援圆摇鉴别的方法 …… 圆

员援员援猿摇人类用户鉴别 …… 猿

员援员援源摇鉴别的阶段 …… 缘

员援员援缘摇可信任第三方的参与 …… 缘

摇员援圆摇身份鉴别系统 运葬怎遭藻则燥泽 …… 愿

员援圆援员摇运葬怎遭藻则燥泽介绍 …… 愿

员援圆援圆摇运葬怎遭藻则燥泽的目的 …… 怨

员援圆援猿摇运葬怎遭藻则燥泽协议 …… 员园

员援圆援源摇运葬怎遭藻则燥泽模型 …… 员园

员援圆援缘摇运葬怎遭藻则燥泽工作原理 …… 员园

员援圆援远摇运葬怎遭藻则燥泽第缘版与第源版的区别 …… 员猿

员援圆援苑摇运葬怎遭藻则燥泽的安全性 …… 员源

摇员援猿摇公开密钥基础设施 …… 员源

员援猿援员摇概述 …… 员源

员援猿援圆摇孕运陨提供的服务 …… 员怨

员援猿援猿摇孕运陨构成 …… 圆员

员援猿援源摇孕运陨标准 …… 圆源

员援猿援缘摇基于孕运陨的信任模型 …… 圆缘

[illegible]的运行模型 …… 32
[illegible]公钥基础设施 …… 34

2 防火墙技术 …… 47

2.1 基本概念 …… 48
2.2 防火墙的基本类型 …… 49
2.2.1 包过滤 …… 49
2.2.2 应用网关 …… 51
2.2.3 电路网关 …… 52
2.2.4 混合型防火墙 …… 53
2.2.5 状态检测防火墙 …… 54
2.3 防火墙的配置形式 …… 56
2.3.1 包过滤路由器防火墙 …… 56
2.3.2 双穴机网关防火墙 …… 57
2.3.3 主机过滤防火墙 …… 57
2.3.4 子网过滤防火墙 …… 58
2.3.5 跨越公共网络的基于[illegible]的内联网防火墙系统 …… 59
2.4 防火墙的局限性 …… 60
2.5 防火墙的应用示例 …… 61
2.5.1 主要特性 …… 61
2.5.2 典型应用配置实例 …… 63

3 入侵检测 …… 71

3.1 入侵检测系统概述 …… 72
3.1.1 入侵检测系统的功能 …… 72
3.1.2 入侵检测的发展 …… 72
3.1.3 入侵检测系统的分类 …… 73
3.2 入侵检测系统的系统结构 …… 75
3.2.1 [illegible]模型 …… 75
3.2.2 简单的分布式入侵检测系统 …… 76
3.2.3 基于智能代理技术的分布式入侵检测系统 …… 77
3.3 入侵检测分析技术 …… 79
3.3.1 入侵分析概述 …… 79
3.3.2 异常检测分析方法 …… 81
3.3.3 滥用检测分析方法 …… 83
3.4 入侵检测系统的实际应用 …… 87

猿援缘援圆 陨阅杂的部署 …… 愿苑
猿援缘援猿 入侵检测系统存在的问题和发展方向 …… 怨园
猿援缘援源 典型入侵检测系统简介 …… 怨猿

源揺灾孕晕与网络安全 …… 怨愿

揺源援员揺前言 …… 员园园
揺源援圆揺灾孕晕技术及其应用 …… 员园员
源援圆援员揺灾孕晕概念 …… 员园员
源援圆援圆揺灾孕晕技术的发展 …… 员园圆
源援圆援猿揺灾孕晕的应用领域 …… 员园圆
揺源援猿揺灾孕晕技术及其管理 …… 员园缘
源援猿援员揺灾孕晕在 栽悦孕/陨孕协议栈的实现 …… 员园缘
源援猿援圆揺灾孕晕的管理问题 …… 员园苑
揺源援源揺灾孕晕与网络安全 …… 员员园
源援源援员揺网络安全的要素 …… 员员园
源援源援圆揺安全 灾孕晕与网络安全 …… 员员缘
揺源援缘揺链路层隧道封装技术 …… 员员苑
源援缘援员揺孕孕栽孕协议 …… 员员苑
源援缘援圆揺蕴圆栽孕协议 …… 员员苑
源援缘援猿揺蕴圆云协议 …… 员员愿
揺源援远揺因特网协议安全 …… 员员愿
源援远援员揺概述 …… 员员愿
源援远援圆揺设计 陨孕泽藻糟的目的 …… 员员愿
源援远援猿揺陨孕泽藻糟的体系结构 …… 员员怨
揺源援苑揺杂杂蕴和 栽蕴杂 …… 员圆远
源援苑援员揺杂杂蕴 …… 员圆远
源援苑援圆揺栽蕴杂 …… 员猿愿
源援苑援猿揺杂杂蕴的应用 …… 员猿猿

缘揺因特网应用安全 …… 员猿员

揺缘援员揺宰宰宰的安全 …… 员猿园
缘援员援员揺宰宰宰安全分析 …… 员猿园
缘援员援圆揺宰藻遭安全防护技术 …… 员猿苑
缘援员援猿揺主页防黑技术 …… 员猿怨
揺缘援圆揺电子商务的安全 …… 员源员
揺缘援猿揺因特网信息过滤技术 …… 员源缘

缘援缘援员摇内容阻塞 …… 员远源
缘援缘援圆摇内容定级和自我鉴定 …… 员远缘
缘援缘援猿摇砸粤悦蕴 …… 员远愿
缘援缘援源摇使用内容定级和自我鉴定的例子 …… 员苑园
缘援缘援缘摇其他一些客户端封锁软件 …… 员苑园
摇缘援远摇电子邮件的安全 …… 员苑猿
缘援远援员摇概述 …… 员苑猿
缘援远援圆摇孕郧孕 …… 员苑缘
缘援远援猿摇杂酝陨酝耘 …… 员苑苑
缘援远援源摇垃圾邮件 …… 员愿员
摇缘援苑摇网上数据库安全 …… 员愿源
缘援苑援员摇数据库系统 …… 员愿源
缘援苑援圆摇数据库基本安全架构 …… 员愿缘
缘援苑援猿摇数据库的安全控制 …… 员愿远
缘援苑援源摇数据库加密 …… 员愿苑
缘援苑援缘摇韵则葬糟造藻数据库的安全措施 …… 圆园员

远摇安全审计和报警 …… 圆园缘

摇远援员摇基本概念 …… 圆园远
摇远援圆摇安全审计线索 …… 圆园苑
摇远援猿摇开放系统互联的安全审计和报警通则 …… 圆园愿
摇远援源摇审计事件的时间注册 …… 圆员园
摇远援缘摇安全审计和报警功能及实现 …… 圆员员
远援缘援员摇安全审计和报警准则 …… 圆员员
远援缘援圆摇安全审计和报警模型的实现 …… 圆员圆
远援缘援猿摇安全审计和报警设施概览 …… 圆员源
远援缘援源摇安全审计的日常管理 …… 圆员缘
远援缘援缘摇安全审计与反制 …… 圆员缘
远援缘援远摇审计实现和应用时的若干考虑 …… 圆员远

苑摇病毒与恶意代码 …… 圆圆猿

摇苑援员摇概述 …… 圆圆源
苑援员援员摇病毒的由来 …… 圆圆源
苑援员援圆摇计算机病毒在中国 …… 圆圆远
摇苑援圆摇计算机病毒的特点与种类 …… 圆圆远
苑援圆援员摇计算机病毒的特点 …… 圆圆远

殑援援摇关于计算机病毒的分类 …………………………………………………… 圆苑
摇殑援猿摇病毒的产生、传播途径和寄生软件 ………………………………………… 圆愿
殑援猿援员摇病毒的产生 …………………………………………………………… 圆愿
殑援猿援圆摇病毒的传播途径 ………………………………………………………… 圆怨
殑援猿援猿摇病毒的寄生软件 ………………………………………………………… 猿园
摇殑援源摇计算机病毒的结构和形式描述 ……………………………………………… 猿员
殑援源援员摇计算机病毒的结构 ……………………………………………………… 猿员
殑援源援圆摇计算机病毒的形式描述 …………………………………………………… 猿员
摇殑援缘摇病毒的表现行为 ……………………………………………………………… 猿猿
摇殑援远摇典型病毒简介 ………………………………………………………………… 猿源
摇殑援苑摇计算机病毒的动态特性 ……………………………………………………… 猿苑
摇殑援愿摇反病毒的斗争 ………………………………………………………………… 猿怨
殑援愿援员摇提高认识 …………………………………………………………… 猿怨
殑援愿援圆摇建立、健全法律法规和管理制度,加强教育和宣传 ………………… 猿怨
殑援愿援猿摇病毒防范的技术措施 ……………………………………………………… 源园
愿摇黑客、黑客技术及其防范措施 ……………………………………………………… 源缘
摇愿援员摇什么是黑客 ……………………………………………………………………… 源远
愿援员援员摇黑客的定义和分类 ……………………………………………………… 源远
愿援员援圆摇黑客对网络信息系统的影响 ……………………………………………… 源员
愿援员援猿摇相关法律 …………………………………………………………………… 源员
摇愿援圆摇黑客常用的攻击方法和防范措施 ……………………………………………… 源猿
愿援圆援员摇黑客攻击的一般过程 …………………………………………………… 源猿
愿援圆援圆摇信息探测 …………………………………………………………………… 源源
愿援圆援猿摇网络嗅探攻击技术 ……………………………………………………… 缘圆
愿援圆援源摇缓冲区溢出攻击 ………………………………………………………… 缘愿
愿援圆援缘摇杂韵蕴注入式攻击 ……………………………………………………… 远园
愿援圆援远摇特洛伊木马攻击技术 ……………………………………………………… 远猿
摇愿援猿摇黑客技术的可利用性 ……………………………………………………………… 苑园
愿援猿援员摇利用黑客技术对信息系统进行监管 ………………………………………… 苑园
愿援猿援圆摇促进对黑客技术的研究和利用 ……………………………………………… 苑员
怨摇信息系统安全方案设计方法 …………………………………………………………… 苑猿
摇怨援员摇信息系统基本结构及资源分析 ……………………………………………… 苑源
怨援员援员摇网络结构 …………………………………………………………………… 苑源
怨援员援圆摇资源分析 …………………………………………………………………… 苑缘

摇怨愿摇安全风险分析 …… 圆愿怨
怨愿员摇安全事件发生可能性 (概率) 分析 …… 圆愿怨
怨愿圆摇攻击者及其目的分析 …… 圆愿怨
怨愿猿摇攻击地点及其工具分析 …… 圆园员
怨愿源摇脆弱性分析 …… 圆园员
怨愿缘摇攻击结果分析 …… 圆园圆
怨愿远摇用户风险分析 …… 圆园圆
怨愿苑摇支持系统风险分析 …… 圆园猿
怨愿愿摇残余风险分析 …… 圆园猿
摇怨怨摇安全需求分析 …… 圆园猿
怨怨员摇按对信息的保护方式进行安全需求分析 …… 圆园源
怨怨圆摇按与风险的对抗方式进行安全需求分析 …… 圆园缘
摇怨苑摇安全规则与设计原则 …… 圆园远
摇怨愿摇系统安全体系 …… 圆园苑
怨愿员摇技术体系 …… 圆园愿
怨愿圆摇组织体系 …… 圆员怨
怨愿猿摇管理体系 …… 猿员员
摇怨怨摇安全解决方案 …… 猿员员
怨怨员摇安全方案总成 …… 猿员员
怨怨圆摇物理安全和运行安全 …… 猿员圆
怨怨猿摇网络规划与子网划分 …… 猿员猿
怨怨源摇网络隔离与访问控制 …… 猿员源
怨怨缘摇操作系统安全增强 …… 猿员苑
怨怨远摇应用系统安全 …… 猿员怨
怨怨苑摇重点主机防护系统 …… 猿圆员
怨怨愿摇连接与传输安全 …… 猿圆猿
怨怨怨摇安全综合管理与控制 …… 猿圆苑
附录 …… 猿猿怨
摇附录 员摇信息安全常用缩略语 …… 猿猿员
摇附录 圆摇名词与术语 …… 猿猿怨
参考文献 …… 猿源源

1

身份鉴别技术

员援猿摇身份鉴别

员援猿援员摇鉴别的基本概念

鉴别技术是访问控制和授权操作等安全服务的前提,需要利用它来证实其所声称的身份和数据来源的真实性。鉴别服务可提供对通信中实体身份和数据来源的两种鉴别。

所谓实体鉴别是指当该服务由(晕)层提供时,将使(晕垣员)层实体确信与之打交道的实体正是它所需的(晕垣员)实体。例如,网络上圆台主机在同等分层上建立连接,或数据传输过程中对对方实体的合法性进行鉴别以防假冒。对等实体可以是用户与用户、进程与进程,或它们的组合,如客户与服务器、服务器与服务器等等。

鉴别服务通常在连接建立或在数据传送阶段的某些时刻提供使用,用以证实一个或多个连接实体的身份。使用实体鉴别服务可以确信(仅在使用时间内):一个实体此时没有试图冒充别的实体。

实施单向或双向对等实体鉴别也是有可能的,可以带有效期检验,也可以不带。

鉴别服务的另一种形式是数据原发鉴别,这种鉴别服务当由(晕)层提供时,将使(晕垣员)实体确信数据来源正是所要求的对等(晕垣员)实体。也就是说,数据原发鉴别服务对数据单元的来源提供识别。这种服务对数据单元的重复或篡改不提供保护。

数据原发鉴别通常是在两个通信实体之间建立连接后,每个通信实体对收到的信息的来源进行验证,以确保所收到信息的来源的真实性的过程。

总而言之,鉴别是保证通信中实体和信息来源真实性的一个过程,鉴别技术的共性是对某些参数(例如身份标识和数据来源的信息等)的有效性进行检验,即检查这些参数是否满足某些事先预定的关系或特征。

员援猿援圆摇鉴别的方法

鉴别为判定一个实体所宣称身份提供确认。只有在主体和验证者的关系背景下,鉴别才是有意义的,其中主体是被鉴别的实体。有圆种重要的关系背景:一是主体由申请者来代表,申请者与验证者之间存在着特定通信关系(实体鉴别),这里的"通信关系"可以有广义的解释,例如它可指韵杂陨连接、内部进程通信,或用户与终端的交互;二是主体是提供给验证者的源数据项(数据源鉴别)。

在通信关系背景下,实体鉴别提供了对主体身份的确认。主体的已鉴别身份仅在服务被请求时才被保证。实体鉴别只对鉴别时刻的身份提供确认保证,获得鉴别持续性保证的方法是将该鉴别服务与数据完整性服务结合起来。

实体鉴别有下列几种方法:

①验证实体已知什么,如一个口令或秘密的通行字。

②验证实体拥有什么,如通行证、智能 陨鼠卡。

③验证实体不可改变的特性,如指纹、声音等生物学测定得来的标识特征。

④相信可靠的第 猿方建立的鉴别(递推)。

⑤环境(如主机地址)。

注意 :通过“拥有”某物进行鉴别,一般是鉴别拥有的东西而不是鉴别拥有者。它是否由一个特定主体所惟一拥有,是此方法的关键所在,也是此方法的不足之处。在第④项中,有 圆种递推方式 :第 员种,第 猿方可能自己要求被鉴别 ;第 圆种,第 猿方建立的鉴别可使用第 源方。一般来说,特别的鉴别方法也要依靠与某一原理相关的假定或估计,因此就形成了逻辑论证。通过论证,使用这种方法的人可以验证其已鉴别的实体身份。论证必须在使用某种方法之前进行,如果不预先论证或未公布论证方法,使用这种方法所导致的风险可能比预料的大得多。

数据源鉴别提供对特定数据单元负责的该主体身份的确认。使用数据源鉴别时,必须充分保证源数据未被修改,这可以通过完整性服务完成。例如:

①通过使用数据不可被改变的环境。

②通过验证所收到数据与发送数据的数字指纹的匹配。

③通过使用数字签名机制。

④通过使用对称密码算法。

员援猿援圆 人类用户鉴别

当开放系统支持人类活动时,人类用户与计算机系统间的对话增加了冒充者入侵的可能性,为此,系统最终要鉴别的必须是人类用户而不是代表人类用户行为的进程。因此,正确的人类用户鉴别在该开放系统中是必须的。人类用户的鉴别方法必须令人类用户可以接受,同时也应该是经济和安全的,否则会导致人类用户寻求回避鉴别过程的种种途径,从而导致潜在入侵威胁的增加。

人类用户的鉴别可有以下几类方法:

①验证已知事物。

②验证所持有的事物。

③验证人类用户的生物特征。

④接受已验明的可信任第 猿方所建立的人类用户身份。

员 通过已知某物鉴别

这是一种最常用也是最简单的鉴别方法。在该鉴别类型中,最常用的鉴别信息是口令或通行字。当人类用户访问一个系统时,访问者必须出示口令,而鉴别系统将它与口令清单中的相应值比较,从而确认该人类用户的身份。口令应该难于猜测,并被