



Information
Security Management
Handbook
(Volume III)
Fourth Edition

信息安全 管理手册(卷III) (第四版)

[美] Harold F. Tipton Micki Krause 主编
张文 邓芳玲 程向莉 吴娟 译



电子工业出版社

PUBLISHING HOUSE OF ELECTRONICS INDUSTRY

<http://www.phei.com.cn>

电子信息科技专著出版专项资金资助出版

信息安全手册（卷Ⅲ）

（第四版）

Information Security Management Handbook(Volume3)
Fourth Edition

[美] Harold F. Tipton Micki Krause 主编

张 文 邓芳玲 程向莉 吴 娟 译

Publishing House of Electronics Industry

北京 • BEIJING

内 容 简 介

随着科学技术的迅猛发展,信息安全人员面临着越来越大的挑战。本书汇集了各种技术的最新发展趋势、新概念以及相应的安全管理方法,系统、全面地阐述了与信息安全管理相关的内容。全书分为10部分,内容包括:访问控制系统和方法,电信和网络安全,安全管理实践,应用程序和系统开发的安全性,密码术,安全结构和模型,操作安全,商业持续性计划和灾难恢复计划,法律、调查和道德标准,以及物理安全。

本书既适合作为参加 CISSP 证书考试的教材,又适合信息安全技术人员和管理人员用做日常参考手册。

Information Security Management Handbook, Fourth Edition, Volume III, Copyright 2002, CRC Press LLC

本书中文简体版专有出版权由 CRC Press 授予电子工业出版社,未经许可,不得以任何方式复制或抄袭本书的任何部分。

版权贸易合同登记号 图字:01-2002-5473

图书在版编目(CIP)数据

信息安全管理手册.3卷:第4版/(美)泰普顿(Tipton, H.F.), (美)克劳斯(Krause, M.)著;张文, 邓芳玲, 程向莉译. —北京:电子工业出版社, 2004. 6

书名原文: Information Security Management Hand book

ISBN 7-5053-00044-6

I. 信… II. ①泰…②克…③张…④邓…⑤程… III. 信息系统—安全管理—技术手册 IV.TP309-62

中国版本图书馆 CIP 数据核字(2004)第 046361 号

责任编辑:张来盛

印 刷:北京民族印刷厂

出版发行:电子工业出版社

北京市海淀区万寿路 173 信箱 邮编 100036

经 销:各地新华书店

开 本:787×1092 1/16 印张:28.5 字数:728 千字

印 次:2004 年 6 月第 1 次印刷

印 数:5 000 册 定价:52.00 元

凡购买电子工业出版社的图书,如有缺损问题,请向购买书店调换。若书店售缺,请与本社发行部联系。联系电话:(010) 68279077。质量投诉请发邮件至 zltts@phei.com.cn, 盗版侵权举报请发邮件至 dbqq@phei.com.cn。

译者序

网络信息安全在国家信息化建设过程中占据非常重要的地位,经过十多年的飞速发展,网络已成为我国与世界进行信息交流的主要手段。网络上信息资源的安全性就显得格外重要,尤其对一些相当重要的数据、资料的安全保护已成为网络安全管理的必然趋势。网络的快速发展是国家信息化发展的前提,而信息安全管理已成为当前网络发展的主要切入点。因此,采用何种保护手段、运用哪些保护措施以及应该保护哪些内容,成为网络安全管理的主要研究内容。

网络信息安全是一项动态的、整体的系统工程,从技术上来说,网络信息安全由安全的操作系统、应用系统、防病毒、防火墙、入侵检测、网络监控、信息审计、通信加密、灾难恢复、安全扫描等多个安全组件组成,一个单独的组件是无法确保信息网络的安全性的。

本书重点针对一些普遍性问题和所应采用的相应安全技术,系统、全面地介绍了信息安全管理的相关技术、设备、应用和防范措施。本书具有以下显著特点:

(1) 权威经典。本书原作者是美国长期从事网络安全研究、设计和标准制定的知名专家,已有多部关于网络安全的专著出版。其内容构成了系统的理论体系,在学术上具有国际领先水平,又涵盖了最新的网络安全技术,具有相当的权威性。

(2) 全面、系统。本书篇幅较大,覆盖面广,内容涵盖了网络技术的方方面面和相关的标准,是目前信息安全管理类书籍中“最全面、最系统的一本技术专业书籍”。

(3) 技术先进,具有现实性和前瞻性。本书密切结合实践,注重技术的先进性,对当今网络发展中的新技术和新应用,如生物测量学、远程通信和网络安全、ERP的安全、注册信息表的安全、物理层的安全、网络层的安全、安全的操作系统、应用系统、防病毒、防火墙、入侵检测、网络监控、信息审计、通信加密、灾难恢复、安全扫描等,都进行了系统阐述。

(4) 内容新颖,具有独创性。本书循序渐进,深入浅出,层次清楚,详简得当,按照不同研究领域分开叙述,从一般到特殊、由基本到全面进行讲述。各篇相互独立,自成体系,以满足不同的读者需求。

(5) 理论与实践紧密结合。本书既有丰富的基本理论,又汇集了多年来网络安全发展的最新经验,对于网络安全管理的工程设计、系统维护等实践都具有重要的指导作用和较高的应用价值。

(6) 实例、资料丰富。本书提供了大量的实例和技术资料,可使读者举一反三,推广、应用到具体工程实践中去。

本书概括了目前美国IT业界对网络安全管理的建设经验,从网络安全的保护手段、保护措施、保护的内容出发进行详尽的分析,对提高现有网络质量,确保网络安全,开展新业务,以及帮助领导决策都将起到新的作用。

本书主要由张文、邓芳玲、程向莉、吴娟翻译,参加翻译的还有邢淑琴、杨弃、吴春清、卢醒春、陈春生、俞海莹、汤志强、张明安等,在本书翻译过程中,邵自力研究员、吴吉祥研究员给予了亲切指导。在此表示感谢。

由于译者水平有限,不妥之处在所难免,恳请读者指正。

前 言

信息技术的迅猛发展，使信息安全专业人员面临着越来越大的挑战。因此，我们很高兴将《信息安全管理手册》（第四版）的第3卷奉献给广大读者，其中讲述了不断发展的技术的形成趋势、新概念以及安全方法，旨在为信息安全人员提供最新内容的日常参考手册——这也是我们不变的承诺。

再者，我们根据信息安全知识共同体（CBK）的要求不断调整《信息安全管理手册》的内容，以便为信息安全专业人员准备 CISSP 证书考试提供参考资料。CISSP 证书考试和 CBK 研究班课程由国际信息系统安全证书联盟（(ISC)²）举办，世界各地都在开展，而且具有很大的需求。

准备 CISSP 证书考试需要付出巨大的努力，这是因为它要求全面理解和应用 CBK 中所包含的主题。《信息安全管理手册》系列图书被认为是准备 CISSP 证书考试的应试者使用的一种最重要的参考书。技术人员在日常工作中也使用这些图书，他们经常要用到书中所提供的实践信息。

面对计算机病毒和蠕虫的不断增殖，以及恶意黑客利用开放网络协议的安全漏洞而发起的威胁，勤勉的首席执行官（CEO）们（他们有责任保护公司的资产）不得不聘用最高素质的安全职员。因此，同以前相比，如今在招聘时更要求有 CISSP 指定证书。

这一版《信息安全管理手册》及其将来版本，特意将内容按照 CISSP 证书考试的各部分进行编排。每本书都有一章或几章讲述宽范围的信息安全领域中所包含的特定 CBK 主题。因此，我们的目的是保持在每一版中都有一些全新的章节，以确保书中的内容随着信息安全领域的技术发展而保持同步。同以前的版本相比，这一版任何一章内容都不重复。

Harold F. Tipton
Micki Krause

目 录

第 1 部分 访问控制系统和方法

第 1 章 生物测量学：有哪些新技术	(2)
1.1 指纹	(2)
1.2 眼睛扫描	(2)
1.3 面部识别	(2)
1.4 手和声音	(3)
1.5 生物测量学新技术	(3)
1.6 微软	(4)
1.7 标准化问题	(5)
1.8 选择准则	(5)
1.9 结论	(5)
第 2 章 医护行业中的隐私问题	(7)
2.1 引言	(7)
2.2 HIPAA	(10)
2.3 其他的病人隐私法	(12)
2.4 实施新隐私法的技术挑战	(12)
2.5 结论	(16)
第 3 章 新一代黑客工具及防卫方法	(17)
3.1 分布式攻击	(17)
3.2 动态嗅探	(22)
3.3 内核级 RootKit 的增殖	(26)
3.4 结论	(28)
第 4 章 社交工程——被遗忘的危险	(29)
4.1 引言	(29)
4.2 社交工程的定义	(29)
4.3 为什么社交工程起作用	(30)
4.4 社交工程的攻击	(31)
4.5 减小危险	(32)
4.6 对付社交工程的保护机制	(33)
4.7 概括	(34)
4.8 防卫社交工程的攻击	(34)
4.9 结论	(36)

第 2 部分 电信和网络安全

第 5 章 安全和网络技术	(38)
---------------------	------

5.1	网络是什么	(38)
5.2	网络设备	(38)
5.3	网络类型	(39)
5.4	网络拓扑	(40)
5.5	网络格式	(44)
5.6	线缆类型	(49)
5.7	电缆损坏	(50)
5.8	结论	(51)
第 6 章	有线和无线物理层安全问题	(52)
6.1	有线网络拓扑基础	(52)
6.2	共享集线器	(53)
6.3	交换集线器扩展物理安全	(53)
6.4	虚拟局域网的不可信安全	(54)
6.5	VLAN/子网加交换	(55)
6.6	物理配线安全	(55)
6.7	无线物理层安全	(56)
6.8	结论	(57)
第 7 章	网络路由器安全	(58)
7.1	路由器硬件和软件构成	(58)
7.2	控制数据流	(60)
7.3	配置路由器	(60)
7.4	路由器访问列表	(62)
7.5	结论	(65)
第 8 章	无线 Internet 的安全	(66)
8.1	谁使用无线 Internet	(66)
8.2	有什么类型的应用	(67)
8.3	传输方法的安全性如何	(67)
8.4	无线设备的安全性	(70)
8.5	网络基础设施部分的安全性如何	(72)
8.6	结论	(76)
	参考文献	(77)
第 9 章	虚拟专用网 (VPN) 的利用和评价策略	(78)
9.1	VPN 是什么	(78)
9.2	IPSec VPN 应用	(78)
9.3	保证内部网络的安全	(84)
9.4	VPN 开发模式	(85)
9.5	VPN 性能评价	(87)
9.6	VPN 外包	(89)
9.7	总结	(90)

词汇表.....	(90)
第 10 章 如何完成检查站防火墙的安全检查	(92)
10.1 防火墙检查的必要性	(92)
10.2 检查、核查和评价	(92)
10.3 防火墙检查的步骤	(92)
10.4 结论	(103)
第 11 章 防火墙技术比较	(104)
11.1 防火墙技术	(105)
11.2 边界防御和防火墙如何配置	(107)
11.3 总的建议和结论	(110)
第 12 章 虚拟专用网的安全	(111)
12.1 首要问题	(111)
12.2 漫游用户	(111)
12.3 Internet 的采用	(113)
12.4 宽带	(113)
12.5 扩展访问	(114)
12.6 始终连接	(114)
12.7 访问公司网络	(115)
12.8 结束开放	(116)
12.9 访问点	(117)
12.10 安全的封装	(117)
12.11 易攻击性概念	(118)
12.12 退步	(119)
12.13 案例	(121)
12.14 解决方案	(122)
12.15 结论	(122)
第 13 章 E-mail 安全	(124)
13.1 目标和无目标	(124)
13.2 E-mail 通信的特定风险和问题	(125)
13.3 E-mail 内容特定的风险和问题	(128)
13.4 无线安全	(130)
13.5 E-mail 安全工具	(131)
13.6 更新	(131)
13.7 小结	(131)
第 14 章 Cookie 和 Web bug: 它们是什么以及如何一起工作.....	(132)
14.1 Cookie 是什么	(132)
14.2 Cookie 的内容	(132)
14.3 Cookie 的正面性	(134)
14.4 Cookie 的负面问题	(135)

14.5	Web bug 是什么	(136)
14.6	Web bug 的隐私和其他问题	(136)
14.7	Web bug 和 Cookie 的同步	(136)
14.8	小结	(137)
第 15 章	利用虚拟专用网	(138)
15.1	VPN 的关键优势	(138)
15.2	融合的网络	(139)
15.3	WAN 卸载	(143)
15.4	结论	(146)
第 16 章	无线 LAN 安全	(147)
16.1	标准	(147)
16.2	安全问题	(147)
16.3	默认安装	(148)
16.4	降低风险	(148)
16.5	MAC 地址	(148)
16.6	服务组标识符	(148)
16.7	有线对等加密 (WEP)	(148)
16.8	认证解决方案	(149)
16.9	第 3 方产品	(149)
16.10	网关控制	(149)
16.11	结论	(150)

第 3 部分 安全管理实践

第 17 章	维持经理的承诺	(152)
17.1	“你最近为我做了些什么?!”	(152)
17.2	交流	(152)
17.3	会议	(154)
17.4	教育	(155)
17.5	激励因素	(157)
17.6	小结	(159)
第 18 章	加强安全意识	(160)
18.1	确立目标	(161)
18.2	确定具体的内容	(161)
18.3	实施 (发布) 选项	(161)
18.4	克服困难	(163)
18.5	评估	(163)
18.6	小结	(164)
18.7	培训	(164)
18.8	总结	(169)

第 19 章 加强安全意识: 附录	(171)
19.1 培训方略 (培训内容发布的模式)	(171)
19.2 推荐的 IT 系统安全培训课程	(172)
第 20 章 策略的制定	(179)
20.1 组织机构文化的影响	(179)
20.2 安全策略的发展历史	(179)
20.3 为什么需要策略	(182)
20.4 管理职责	(183)
20.5 为策略做计划	(185)
20.6 策略管理层次	(185)
20.7 策略的类型	(186)
20.8 编写策略	(187)
20.9 定义标准	(190)
20.10 定义规程	(190)
20.11 定义方针	(191)
20.12 发布策略	(192)
20.13 建立一个通用格式	(192)
20.14 使用一个通用的制订过程	(194)
20.15 总结	(196)
参考文献	(196)
第 21 章 信任问题	(197)
21.1 信任问题	(197)
21.2 保护基础结构	(202)
21.3 风险管理 101	(203)
21.4 底线	(207)
21.5 赢得信任	(207)
致谢	(208)
参考文献	(208)
第 22 章 风险管理和分析	(211)
22.1 定量风险分析	(212)
22.2 定性风险分析	(213)
22.3 要点	(215)
22.4 风险管理	(216)
22.5 小结	(217)
第 23 章 信息风险管理的新趋势	(218)
23.1 传统方法	(218)
23.2 尽力做到最好	(218)
23.3 相关常识: 怎样进行防护	(219)
23.4 业务连续性管理	(220)

23.5	重新进行企业的防护工作	(221)
23.6	小结	(223)
第 24 章	企业的信息安全性	(225)
24.1	安全需求: 访问公司数据	(225)
24.2	信息安全需求	(226)
24.3	主要的安全功能	(226)
24.4	IT 需求	(228)
24.5	加密: 实现安全性的关键因素	(229)
24.6	企业安全框架的实施	(232)
24.7	选择技术供应商	(234)
24.8	实施以及测试	(235)
24.9	小结	(236)
第 25 章	企业安全信息管理	(237)
25.1	企业安全性信息来源	(237)
25.2	入侵检测系统	(239)
25.3	防火墙类型及其在加强安全方面的作用	(243)
25.4	操作系统日志	(245)
25.5	路由器及交换机	(247)
25.6	企业信息管理的策略	(248)
25.7	安全漏洞数据	(251)
25.8	小结	(251)
	参考文献	(252)
第 26 章	配置管理	(253)
26.1	系统安全工程能力成熟模型 (SSE-CMM) 概述	(253)
26.2	安全工程	(256)
26.3	配置管理	(257)
26.4	配置管理的基础实践	(258)
26.5	建立配置管理方法	(258)
26.6	识别控制单元	(260)
26.7	维护工件基线	(262)
26.8	控制已建立的配置单元的变更	(262)
26.9	交流配置状态	(264)
26.10	小结	(266)

第 4 部分 应用程序及系统开发的安全性

第 27 章	Web 应用程序的安全性	(270)
27.1	Web 应用程序的安全性	(270)
27.2	跨站脚本执行	(272)
27.3	参数篡改	(272)

27.4	cookie 中毒	(272)
27.5	输入操作	(273)
27.6	缓冲区溢出	(273)
27.7	直接存取浏览	(273)
27.8	防护措施	(273)
27.9	技术工具及解决方案	(275)
27.10	小结	(276)
第 28 章	理想状态下的安全体系	(281)
28.1	构造完美的安全体系	(282)
28.2	法律法规: 策略、方法、标准及准则	(285)
28.3	周边安全 (⑩)	(286)
28.4	台式机	(286)
28.5	网络	(287)
28.6	服务器和主机	(287)
28.7	应用程序	(288)
28.8	数据库	(288)
28.9	小结	(289)
第 29 章	XML 及其他元数据语言的安全性	(290)
29.1	元数据	(290)
29.2	万维网的安全性	(295)
29.3	推荐做法	(296)
29.4	小结	(297)
	参考文献	(297)
第 30 章	XML 以及信息的安全性	(298)
30.1	XML 基础	(298)
30.2	HTML 的局限性	(298)
30.3	其他 XML 工具	(301)
30.4	XML 的安全问题	(302)
30.5	小结	(304)
第 31 章	关系数据库应用程序中的数字签名	(306)
31.1	数字签名的基本概念	(306)
31.2	不同的数据库	(308)
31.3	集成方法	(310)
31.4	关系数据库中数字签名的通用方法	(312)
31.5	小结	(314)
第 32 章	数据仓库的安全和隐私	(315)
32.1	隐私问题概述	(315)
32.2	商业问题	(319)
32.3	支持隐私性的商业需求	(321)

32.4 技术问题	(324)
32.5 小结	(330)
参考文献	(330)

第5部分 密码术

第33章 先进的加密标准 (AES)	(332)
33.1 AES 处理过程	(332)
33.2 AES 候选者	(333)
33.3 Rijndael	(335)
33.4 NIST 为什么选择 Rijndael 码	(335)
33.5 Rijndael 的问题	(335)
33.6 AES 会被解密吗?	(336)
33.7 AES 的影响	(336)
第34章 保存 PKI	(337)
34.1 PKI	(337)
34.2 构建密码安全数字标记 (CSDT)	(339)
34.3 层次分离	(339)
34.4 有 CSDT 证书的发行	(340)
34.5 小结	(341)
参考文献	(342)

第6部分 安全结构和模型

第35章 数据库完整性的思考	(344)
35.1 概念和描述	(344)
35.2 方法	(345)
35.3 结论	(348)
35.4 建议	(348)

第7部分 操作安全

第36章: 智能入侵分析: 四位机怎样能识别计算机的入侵风险	(352)
36.1 为什么有人工智能	(352)
36.2 知识的作用	(353)
36.3 入侵检测的模式匹配方法	(353)
36.4 与入侵检测系统匹配的模式	(356)
36.5 进行中的系统	(359)
36.6 概念的扩展	(362)
36.7 挑战和局限	(363)
36.8 小结	(364)
参考文献	(364)

第 37 章 审查电子商务环境	(365)
37.1 策略	(365)
37.2 合法性	(366)
37.3 隐私	(366)
37.4 出口控制	(367)
37.5 法规	(367)
37.6 项目管理	(368)
37.7 可靠性	(368)
37.8 开发	(371)
37.9 连接性	(371)
37.10 安全性	(372)
37.11 电子商务服务器的安全性	(375)
37.12 操作系统的安全性	(377)
37.13 后台系统应用软件	(378)
37.14 结论	(380)
致谢	(380)

第 8 部分 商业持续性计划和灾难恢复计划

第 38 章 对商业持续性计划流程的再设计	(382)
38.1 持续性计划：高度的管理意识——极差的执行效果	(382)
38.2 接受巨变：CP 流程的改善	(383)
38.3 处理持续性计划的流程方案	(385)
38.4 创造一个 CP 流程的改善环境	(386)
38.5 CP 的价值历程	(388)
38.6 对机构性变化管理的需求	(388)
38.7 如何衡量成功	(389)
38.8 持续性计划在互联网中的应用情况	(391)
38.9 小结	(393)
参考文献	(393)
第 39 章 商业恢复计划和灾难复原：案例历史	(395)
39.1 案例历史	(396)
39.2 专业支持	(399)
39.3 BCP：更新	(401)
39.4 工会	(401)
39.5 风险管理介入	(401)
39.6 裁员	(402)
39.7 文献资料	(402)
39.8 局部处理：谁获得优先	(402)
39.9 注意其他那些会影响最基本恢复点的灾难	(402)

39.10 小结	(403)
参考文献	(403)

第 9 部分 法律、调查和道德标准

第 40 章 发生了什么	(406)
第 41 章 因特网抱怨网站: Bally v. Faber	(410)
41.1 Bally v. Faber 的事实	(411)
41.2 商标法的概述	(411)
41.3 分析: 商标侵犯	(412)
41.4 分析: 商标品牌降低	(413)
41.5 对各企业的建议	(413)
41.6 结论	(413)
参考文献	(413)
第 42 章 对垃圾邮件的控制: Washington v. Heckel	(415)
42.1 案件的事实	(416)
42.2 州际贸易条款	(416)
42.3 Heckel 的分析	(417)
42.4 结论	(418)
参考文献	(418)

第 10 部分 物 理 安 全

第 43 章 物理安全: 信息安全的基础	(420)
43.1 如何着手物理安全	(420)
43.2 物理安全的心理学	(420)
43.3 物理安全设施	(421)
43.4 信息系统的物理安全	(427)
43.5 意识培训	(428)
43.6 小结	(429)
参考文献	(429)
第 44 章 物理安全: 控制访问和层次防卫	(430)
44.1 控制访问	(430)
44.2 物理安全技术	(432)
44.3 物理安全的作用	(434)
44.4 多科学防卫	(434)
44.5 将物理安全与 IT 安全结合成整体的策略	(437)
44.6 物理安全的困难	(437)
44.7 IT 和物理安全的协力合作	(438)
44.8 购买更多的信息	(440)
44.9 小结	(440)

第 1 部分 访问控制系统和方法

倘若认识到信息是无价的而且必须保证信息不被误用、泄露和破坏，很多机构就会实施访问控制，以确保那些用以做出关键商业决定的信息的完整性和安全性。可以采用很多方法控制对计算资源和信息的访问。但是，不管采用什么方法（无论是技术方法还是管理方法），访问控制对一个完善的信息安全系统来说是非常重要的。

这部分讲述用户身份识别和验证，访问控制技术及其管理，以及攻击方法的演变和改进。

生物测量学（生物统计学）用来进行个人身份识别和验证，由于它具有根据一个人的个性特征（如声音、手印、指纹和视网膜图等）准确地识别这个人的能力，因而正迅速成为访问控制的通用方法。虽然生物测量设备已问世多年，但新的方法不断出现。了解了这些重要工具的潜力和局限性，就能合理而有效地应用这些技术。

访问控制的使用没有保护病人健康资料的保密性和安全性重要。在北美之外，特别是欧洲国家，多年来隐私已成为重点。最近美国的消费者要求保护他们的个人隐私，有证据表明他们的医疗信息正成为被泄露的对象。1996 年的 HIPAA 法案（健康保险携带与责任法案）和 1999 年的 Gramm-Leach-Bliley（GLB）法案，证明美国政府正注意到民众的要求。

恶意的攻击正不断地破坏信息控制和降低信息安全性。黑客试图突破一个机构的防卫，而且大多数情况下都获得成功。在本部分中，读者将了解很多先进的现代化攻击工具，这些工具已导致一些广为人知的案例。例如，最近美国司法部的网站被破坏，很多商业网站受到拒绝服务攻击。

社交工程技术是一种利用人的天性很容易就对系统进行控制的方法。在社交工程中，一些无赖采用不正当的办法获得可以用来进行攻击的信息。例如，假扮技术人员给不设防的用户打电话，说需要该用户的网络口令来诊断一个技术问题，然后用该口令来破坏系统。

第 1 章 生物测量学：有哪些新技术

多年来，网络世界的安全建立在口令、个人身份号（PIN）或自己母亲名字之类个人信息基础上。现在可以把生物信息作为补充。生物测量学（生物统计学）从手指、眼睛和面部特征等方面测量一个人，还包括他如何说话和走路的方式等；不久还可以根据一个人的耳朵构成方式以及他如何听取声音来进行测量。

以下简单介绍传统的生物测量学系统以及新的技术和系统。

1.1 指纹

几年之后，用黑墨水获得指纹的方法将过时。人类将进入指尖传感器时代，用指尖触摸传感器可以快速访问远程网络。用户不必担心指纹被仿造，因为没有两个指纹是完全相同的。

指纹由一些纹路组成，包括断点和分岔，就是所说的指纹索引的细节。一个指纹平均有 40~60 个细节。但即使一个指纹模型有足够的细节数，传感器还是有可能无法捕捉所有的细节。对某些人而言，因为每天敲击键盘或弹钢琴，使他们的指纹模型变得很细。另外，如果一个人手指有天生的缺陷或者有疤痕，则他们的指纹模型很难识别。

将指纹模型和登记的指纹对照的方法有 4 种：电子式、热敏式、光学式和混合式传感器。电子式传感器测量指纹高低电场强度。热敏式传感器测量手指接触时指纹凹凸部位的温度差。光学式传感器测量指纹的波长差。混合式传感器是光学式和电子式捕捉设备的结合。

1.2 眼睛扫描

眼睛可以提供几千个细节。指纹细节提供的是外置结构的模型，而眼睛细节提供的是内部结构的模型。可以从两个来源获得这个信息：视网膜和虹膜扫描系统。前者关注视网膜静脉的模型，后者采用虹膜内纤维、组织的模型。

为获得视网膜独特的模型，视网膜扫描仪使用低强度光源，它要求被扫描者往里看并聚焦在一个特定点上。这样对那些戴校正眼镜和不习惯近距离接触者引起不便。

至于虹膜扫描，它使用传统的电视照相设备，无须近距离接触。在光线良好时，这对戴校正眼镜和适当距离接触都工作得很好。一些航线上安装了虹膜扫描仪，以加快旅客登机的过程。

要记住，眼睛模型可能会因为疾病或受伤而发生变化。眼睛扫描仪对盲人和那些视力受损者（尤其是视网膜受损的人）无效。

1.3 面部识别

面部识别系统可以在人出现在电视或闭路摄像头前时自动扫描人的面部。一种新系统工作在暗处，获得面部的热红外模型。赌场已在面部扫描方面投资建立面部数据库，以便保安快速识别作弊高手。