Test and Evaluation on Security of Information Networks

信息网络安全测试与评估

王国良 鲁智勇 等著

国防工业出版社
National Defense Industry Press

信息网络安全测试与评估

王国良　鲁智勇　等著

国防工业出版社
·北京·

内容简介

随着计算机技术和通信技术的发展和网络应用的普及，网络安全问题变得日益重要。认清网络的脆弱性和潜在威胁，采取强有力的安全策略，是保障网络安全的重要途径。通过对网络系统全面、充分、有效的安全评测，能够快速查出网络上存在的安全隐患、网络系统中存在的安全漏洞等。本书从信息网络安全评估指标体系、信息网络安全测试理论、网络攻击分类和建模技术、网络攻防技术、用于网络安全评估的 R_W 转换模型设计和实现、网络安全评估建模等方面对信息网络安全测试和评估理论进行了深入探索和研究。

本书可供从事网络安全和测试人员使用，也可作为高等院校研究生、本科生的教学及工程实践的参考用书。

图书在版编目(CIP)数据

信息网络安全测试与评估/王国良等著. —北京：国防工业出版社，2015.6

ISBN 978-7-118-09645-3

Ⅰ.①信… Ⅱ.①王… Ⅲ.①信息网络－安全评价 Ⅳ.①TP393.08

中国版本图书馆 CIP 数据核字(2015)第 128867 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 100048)

北京嘉恒彩色印刷有限责任公司

新华书店经售

*

开本 710×1000 1/16 **印张** 18½ **字数** 360 千字

2015 年 6 月第 1 版第 1 次印刷 **印数** 1—3000 册 **定价** 58.00 元

(本书如有印装错误，我社负责调换)

国防书店：(010)88540777 发行邮购：(010)88540776

发行传真：(010)88540755 发行业务：(010)88540717

《信息网络安全测试与评估》
编 委 会

编写人员　王国良　鲁智勇　陈　瑞
刘英芝　付海鹏　赵艳丽
毕建权　李志勇

前　言

信息网络安全测试与评估技术的研究，主要是对信息网络安全性进行分析描述、测试与评估，以检验、评估其安全性效果。通过测试，不仅可以分析、评估信息网络在网络攻击环境条件下的安全性，而且还可以在测试中发现和解决问题，并不断消除信息网络存在的缺陷和隐患，从而使信息网络的安全性得到提高和发展。本书从信息网络安全评估指标体系、信息网络安全测试理论、网络攻击分类和建模技术、网络攻防技术、用于网络安全评估的R_W转换模型设计及实现、网络安全评估建模等方面对信息网络安全测试和评估理论进行研究，取得了一系列有价值的研究成果。

(1) 在对网络信息安全要素机密性、完整性和可用性的量化分析基础上，定义了网络安全机密性向量、网络安全完整性向量和网络安全可用性向量，形成了在工程实现中比较可行的网络安全评估指标，建立了层次化信息网络安全评估指标体系。

(2) 提出了集网络漏洞扫描、仿真可信度评估、漏洞树建模、网络攻击、数据采集和网络安全评估于一体的信息网络安全测试框架。

(3) 在对比分析现有网络攻击分类方法的基础上，基于攻击的发起点、所利用的漏洞、取得的权限级别、达到的攻击效果和破坏的安全属性，提出了一种适合于网络安全性测试的网络攻击分类标准体系。

(4) 以目标网络中存在的漏洞为树的叶节点，以漏洞利用攻击方式为节点之间的边，对各个节点主机的安全属性分别进行攻击建模，并在综合分析攻击的成果效率和时间效率的基础上，设计了效率优先的主机安全属性漏洞树建模方法。

(5) 为解决设置有根目录读/写管理权限网络的安全性评估问题，提出了R_W转换模型及其相关概念，然后用状态转换算子⊗对模型转换功能进行了数学描述，设计了基于R_W转换模型的网络安全状态转换器，并以此建立了基于R_W转换模型的网络安全评估模型。

(6) 对于层次分析法(AHP)中不满足一致性要求的判断矩阵，提出了基于预排序和上取整函数的AHP判断矩阵生成算法，此算法在充分利用专家给出的初始判断矩阵信息的基础上，以比较矩阵为基准找出一个既能满足一致性要求、矩阵相异度和调整的元素幅度又较小的目标判断矩阵，又能确保生成目标判断矩阵的元素在1~9及其倒数范围内。在此算法基础上，建立了基于AHP的信息网络安全

定量评估模型。

(7) 为解决有限的测试数据情况下高维 BP 神经网络对于信息网络安全测试评估的训练和预测问题,提出了松弛的和紧密的等效分组级联 BP 神经网络模型等概念,并给出了 BP 神经网络等效性的定义和相关定理,在构建并证明与 BP 神经网络等效的分组级联网络模型的基础上,建立了基于等效分组级联 BP 的信息网络安全评估模型。

本书作者近些年一直致力于网络安全和测试技术的研究和应用,取得了一些研究成果。在撰写此书的过程中,查阅了大量的文献和资料,并将近几年来在理论和工程应用的成果融入有关章节中。编写本书的目的是,促进信息网络安全测试和评估技术的研究,以及开发提供应用思想和可操作性技术。

本书由中国洛阳电子装备试验中心的王国良、鲁智勇、陈瑞、刘英芝、付海鹏、赵艳丽、毕建权及海军航空工程学院的李志勇博士共同撰写,该书的完成体现了团队精神。

本书可作为从事网络安全和测试人员的参考书,也可作为高等院校学生撰写学位论文和工程实践的参考书。

信息网络安全测试与评估是一个崭新的领域,涉及的内容范围又比较广泛,书中难免有不妥之处,敬请广大读者批评指正。

作 者

2015 年 1 月于洛阳

目　录

第1章 绪 论

1.1 引 言

1.1.1 信息安全评估标准

自1985年美国国防部(DoD)发布《可信计算机系统评估准则》(TCSEC)以来,世界各国相继发布了一系列有关安全评估的准则和标准,例如英国、法国、德国、荷兰等国发布的《信息技术安全评估准则》(ITSEC);加拿大发布的加拿大《可信计算机产品评价准则》(CTCPEC);美国发布的《信息技术安全联邦准则》(FC);由加拿大、法国、德国、荷兰、英国及美国国家安全局(NSA)联合提出的《信息技术安全性评估通用准则》(CC);由英国标准协会(BSI)制定的《信息安全管理标准》BS7799以及国际标准化组织(ISO)认可的SSE-CMM(ISO/IEC 21827:2002)等。我国也相继颁布了《计算机信息系统安全保护等级划分准则》(GB 17859—1999)和《信息技术安全性评估准则》(GB/T 18336—2001)等。下面简单介绍其中比较典型的几个标准。

1. 美国的TCSEC

TCSEC(Trusted Computer System Evaluation Criteria)又称橘皮书,1970年由美国国防科学委员会提出,1985年正式发布。起初主要是作为军用标准,后来延伸至民用。其安全级别从高到低分为A、B、C、D四类,各类又进行细分为A1、B3、B2、B1、C2、C1、D7级。分级分类主要依据安全政策、可控性、保证能力和文档的完善程度四个因素。

2. 欧洲的ITSEC

ITSEC(Information Technology Security Evaluation Criteria)1.2版,于1991年由欧洲委员会在结合法国、德国、荷兰和英国的开发成果后公开发表。ITSEC作为多国安全评估标准的综合产物,适用于军队、政府和商业部门。它以超越TCSEC为目的,将安全概念分为功能与评估两部分。功能准则在测定上分F1~F10共10级;评估准则分为6级。

3. 加拿大的评测标准(CTCPEC)

CTCPEC(Canadian Trusted Computer Products Evaluation Criteria)1.0版于1989年公布,专为政府需求而设计,1993年公布了3.0版。作为ITSEC和TCSEC的结合,将安全分为功能性要求和保证性要求两部分。功能性要求分为机密性、完整

性、可用性、可控性等四个大类。在每种安全需求下又分成很多小类，表示安全性上的差别，分级条数为0～5级。

4. 美国联邦准则(FC)

美国《信息技术安全联邦准则(草案)》1.0版也于1993年公开发表，它是结合北美和欧洲有关评估准则概念的另一种标准。在此标准中引入了“保护轮廓(Protection Profile)”这一重要概念，每个轮廓都包括功能部分、开发保证部分和评测部分。其分级方式与TCSEC不同，充分吸取了ITSEC、CTCPEC中的优点，主要供美国政府、民用和商业部门使用。

5. 通用准则(CC)

《信息技术安全性评估通用准则》(Common Criteria of Information Technical Security Evaluation，CCITSE)简称CC，在1993年6月，由与CTCPEC、FC、TCSEC和ITSEC有关的6个国家中7个相关政府组织集中了它们的成果，并联合行动将各自独立的准则集合成一系列单一的、能被广泛接受的IT安全准则。其目的是解决原标准中出现的概念和技术上的差异，并把结果作为对国际标准的贡献提交给了国际标准化组织。1996年颁布了1.0版，1998年颁布了2.0版，1999年6月国际标准化组织正式将CC2.0作为国际标准——ISO 15408发布。在CC中充分突出“保护轮廓”，将评估过程分为“功能”和“保证”两部分。通用准则是目前最全面的信息技术安全评估准则，它由三部分内容组成：①介绍以及一般模型；②安全功能需求(技术上的要求)；③安全认证需求(非技术要求和对开发过程、工程过程的要求)。

CC与早期的评估准则相比，主要具有四大特征：①CC符合保护、检测、响应(Protection Detection Response，PDR)模型；②CC评估准则是面向整个信息产品生存期的；③CC评估准则不仅考虑了保密性，而且还考虑了完整性和可用性多方面的安全特性；④CC评估准则有与之配套的通用评估方法(Common Evaluation Methodology，CEM)。

6. BS7799(ISO/IEC 17799)

BS7799由英国标准协会(BSI)于1995年2月首次公布，1999年5月又进行了修订，是目前国际上最知名的安全管理标准。BS7799的第一部分BS7799－1：1999已于2000年12月被国际标准化组织接纳成为国际标准：ISO/IEC 17799：2000。BS7799由两个部分组成。

第一部分 信息安全实务准则。提供了实现信息安全的全面指导，共列举了10个组织核心领域、127条控制(Control)项目与超过500条的安管细项，以协助组织保护其信息资产。10个核心领域则涵盖了诸如战略方向、人员、访问控制、业务连续性等若干方面的安全策略，甚至防病毒的策略。

第二部分 信息安全管理体系(Information Security Management System，ISMS)规范。提供了一个组织建立、实施及文档化信息安全管理体系的规格说明，ISMS

是实施 BS7799 方法的关键所在。第二部分的新版本 BS7799 - 2:2002 已于 2002 年 9 月完成。该新版本同 ISO 9001:2000(质量管理体系)和 ISO 14001:1996(环境管理体系)等国际知名管理体系标准采用相同的风格,使信息安全管理体系更容易和其他的管理体系相协调。其他主要的修订就是按照规划—实施—检查—行动(Plan - Do - Check - Act. PCDA)模式将信息安全管理体系分解成风险评估、安全设计与实施、安全管理和再评估四个子过程,组织通过持续地执行这些过程而使自身的信息安全水平得到不断的提高。

7. ISO/IEC 21827:2002(SSE - CMM)

信息安全工程能力成熟度模型(System Security Engineering Capability Maturity Model,SSE - CMM),是关于信息安全建设工程实施方面的标准。SSE - CMM 建立和完善一套成熟的、可度量的安全工程过程。该模型定义了一个安全工程过程应有的特征,这些特征是完善的安全工程的根本保证。SSE - CMM 通常以下述三种方式来应用:"过程改善"可以使一个安全工程组织对其安全工程能力的级别有一个认识,于是可设计出改善的安全工程过程,这样就可以提高他们的安全工程能力;"能力评估"使一个客户组织可以了解其提供商的安全工程过程能力;"保证"通过声明提供一个成熟过程所应具有的各种依据,使得产品、系统、服务更具可信性。

8. GB 17859—1999《计算机信息系统安全保护等级划分准则》

1999 年 9 月,我国发布了 GB 17859—1999《计算机信息安全保护等级划分准则》,它是建立安全等级保护制度、实施安全等级管理的重要基础性标准。该标准是我国第一部计算机信息系统保护等级系列标准,该标准的制定参照了美国的 TCSEC,有三个主要目的:一是为计算机信息系统安全法规的制定和执法部门的监督检查提供依据;二是为安全产品的研制提供技术支持;三是为安全系统的建设和管理提供技术指导。

9. GB/T 18336—2001《信息技术安全性评估准则》

自 CC 版公布后,我国相关部门就一直密切关注着它的发展情况,并对该版本做了大量的研究工作。2001 年 3 月,国家质量技术监督局正式颁布了援引 CC 的安全评估 GB/T 18336—2001《信息技术安全性评估准则》。

通过对以上几个主要安全评估标准的比较,可以得出各安全评估标准的特点如下:

(1) TCSEC 对安全的最初定义仅有保密性一点。

(2) ITSEC 首次将安全定义为保密性、完整性与可用性,将功能要求与保证要求分离开来,且其目标在于对产品和系统两者的评估,这些均代表了标准的发展方向。

(3) CTCPEC 在保密性、完整性与可用性基础上又提出了可控性。

(4) BS7799 是侧重于管理理念的最好体现;在对信息系统日常安全管理方

面,BS7799 的地位是其他标准无法取代的,但在安全技术方面不如 CC 分析的系统、透彻。对于 BS7799 来讲,它不是一个技术标准,而是一个管理标准,且它处理的是与已安装的 IT 系统相关的非技术问题。这些问题与人员的、程序上的、物理安全及一般意义上的安全管理等内容有关。

(5) CC 源于 TCSEC,但已经完全改进了 TCSEC。随着信息技术的发展,CC 全面考虑了与信息技术安全性有关的各种因素,并以安全功能要求和安全保证要求的形式提出了这些因素。CC 专注于一个保密性、完整性和可用性的延伸视点,同时它又考虑了可控性、责任可追查性及信息安全的可用性。与 BS7799 相比,CC 旨在支持对产品和系统中 IT 安全特征的规范性与技术性的评估。

(6) SSE - CMM 是系统安全工程领域里成熟的方法体系,在理论研究和实际应用方面具有举足轻重的作用,SSE - CMM 适用于所有从事某种形式安全工程的组织,而不必考虑产品的生命周期、组织的规模、领域及特殊性。它已经成为西方发达国家政府、军队和要害部门组织和实施安全工程的通用方法,我国也准备将 SSE - CMM 作为安全产品和信息系统安全性检测、评估和认证的标准之一。

1.1.2 计算机网络安全评估技术

计算机网络安全评估是一个新兴的研究领域,在各国开展研究的时间还不长,其评估方法也都借鉴装备效能评估等领域的研究成果。装备效能评估方法主要有广义指标法、概率综合法、多属性效用分析法、层次分析法(Analytic Hierarchy Process,AHP)、主成分分析法、模糊综合评估法、基于正负理想点的距离评估方法、最小二乘灰色关联度分析法、集对分析法、灰色聚类评估法、灰色关联分析评估法等。徐德友对当前系统评估工作存在的主要问题进行了分析,指出评估过程的不可重复性、评估标准非标准化、综合评估指标向技术性指标倾斜、效能评估指标的无限定性等是当前面临的主要问题。

网络安全风险评估的方法很多,从数字化的角度,冯登国等人以及王永杰把网络安全评估分为三大类:定量评估方法、定性评估方法、定量与定性相结合的评估方法 ;Ortalo 等人通过使用随机变量描述攻击者进行原子攻击的耗费,并且假设随机变量服从指数分布,建立起了网络系统脆弱性分析的马尔可夫模型,对网络系统脆弱性进行定量评估;Dacier 等人使用随机 Petri 网(Stochastic Petri Nets,SPN)建立网络安全性的定量评估模型;Bharat 等人把攻击行为和系统的反应关联起来,用状态机模型和状态变化的概率评估系统安全性;程克勤等人从网络节点安全评估的各种复杂因素中提取系统的权限作为安全评估的因素,利用矩阵分析网络节点漏洞的权限变化,对漏洞采取漏洞被攻击者发现和漏洞被攻击者成功利用两个方面进行评估,合理地分析了漏洞的属性;张永铮等人提出了一种主机系统安全的量化风险评估方法;陈志杰等人提出了一种利用粗糙集理论挖掘网络安全评估规则,研究了网络安全评估问题的粗糙集描述,给出了模糊属性决策表的约简方法,进而

利用评估规则构建网络安全评估决策系统的算法模型；Sheyner 等人通过攻击图来描述对网络服务、主机漏洞、主机连接关系和远程登录关系等影响网络安全的因素安全状态，把系统及其服务作为评估对象，依据漏洞来分析系统的整体脆弱性；成卫青等参照 CC 的网络安全评估实施框架，重点讨论 TOE（Target of Evaluation）评估依据——安全指标的建立，并给出 EAL1 级和 EAL2 级 TOE 评估的内容；Jha 首先利用攻击图模型进行定性的安全分析，同时，他们将概率值赋予网络攻击中的状态和状态之间的转移，结合马尔可夫决策过程理论，对网络的安全性进行定量分析。王永杰等人利用攻击图对网络系统安全性进行定性或定量分析。

1.1.3 网络攻击分类技术

一直以来，攻击技术作为网络安全领域研究的热点和难点问题，对其进行分析和分类研究，对了解攻击的本质，以更准确地对其进行检测和响应，而且对于研发安全产品、攻击测试网络安全性能等方面都具有重要的意义。

为了判断一个分类方法是否合理并满足实际应用的需求，Amoroso 给出了一个攻击分类方法应满足的分类标准。

（1）完备性：所有可能的攻击都应属于这些类别中的某一类。

（2）确定性（无二义性）：类别划分清晰、明确，不会因人而异。

（3）互斥性：各类别之间不应有重叠。

（4）可重复性：不同人重复分类的过程，得出的分类结果一致。

（5）可接受性：分类符合逻辑和直觉，能得到广泛的认同。

（6）可用性：分类对于该领域的深入研究有实用价值。

（7）适应性：可适应于多个不同的应用要求。

（8）原子性：每个分类无法再进一步细分。

事实上，还没有一个攻击分类方法能够满足以上全部原则，甚至于不能满足主要原则，从已有的分类实践中可以看出人们在研究分类体系时一般重点关注的原则主要有完备性、确定性、互斥性、可重复性、可接受性和可用性。

国外学者在网络攻击分类技术方面取得了一定的研究成果：Cohen 提出将网络攻击分为特洛伊木马、伪造网络资料、冒充、网络探测、溢出电邮、时间炸弹、获取工作资格、刺探保护措施、干扰网络、社会活动、贿赂、潜入、煽动等类型；Icove 按经验将攻击分成病毒和蠕虫、资料欺骗、拒绝服务、非授权资料复制、侵扰、软件盗版、特洛伊木马、隐蔽信道、搭线窃听、会话截持、IP 欺骗、口令窃听、越权访问、扫描、逻辑炸弹、陷门攻击、隧道、伪装、电磁泄露、服务干扰等 20 余类；Neumann 和 Parker 从系统滥用的角度将攻击分为 9 类，即外部滥用、硬件滥用、伪造、有害代码、绕过认证或授权、主动滥用、被动滥用、恶意滥用、间接滥用，并进一步将其细化为 26 种具体的滥用攻击；Stallings 则依据实施方法对网络攻击进行了分类，他将攻击实施的手段归纳为中断、拦截、窃听、篡改和伪造 5 类；Jayaram 也从攻击的实施方法

将网络攻击分成物理攻击、系统弱点攻击、恶意程序攻击、权限攻击和面向通信过程的攻击5类;Cheswick 和 Bellovin 依据攻击后果将针对防火墙的攻击行为分成窃取口令、错误和后门、信息泄漏、协议失效、认证失效、拒绝服务等类别;Alvarez 和 Petrovie 在分析对 Web 应用而发起的攻击时,重点从攻击入口、漏洞、行为、长度、超文本传输协议(Hypertext Transfer Protcol,HTTP)头及动作、影响范围、权限等方面对攻击进行描述,并用不同长度的比特位所代表的数字来表示每一个属性,从而形成一个攻击编码向量;Stephen 等人在对分布式拒绝服务(Distributed Denial of Sevice,DDoS)类攻击进行描述时,对其自动化程度(手动攻击、半自动攻击、自动攻击)、扫描策略(随机扫描、攻击列表扫描、拓扑扫描、本地子网扫描)、传播机制(中心源传播、回溯传播、自治传播)、攻击的漏洞(协议攻击、暴力攻击)、攻击速度的动态性(恒速、变速)、影响(破坏性、降低性能)等属性进行了划分;Weaver 等人从目标发现、策略选择、触发方式等角度对计算机蠕虫进行了描述,提出了一种基于蠕虫目标发现和选择策略、蠕虫传播机制、蠕虫激活方式、蠕虫有效载荷、蠕虫使用者的网络蠕虫分类方法,对于攻击者也按其动机不同进行了划分;Darrell M. Kienzle 和 Matthew C. Elder 对网络蠕虫的概念进行了界定,认为网络蠕虫应该具有以下行为特征:①包含有恶意代码;②通过网络繁殖传播;③不需或很少人工干预;④独立存在或感染依附于其他文件;并将网络蠕虫分为:电子邮件传播、网络文件共享传播和利用网络漏洞传播等三大类;Welch 从使用分析、窃听、中间人攻击、重放攻击等方面描述了针对无线网络的安全攻击;J. Undercoffer 和 J. Pinkston 提出的以攻击目标为核心的攻击描述方法;Man 和 Wei 针对无线代理而发起的攻击进行了描述和分析;Gonzalo álvareza 和 Slobodan Petrovic 对各种 Web 攻击行为的特征进行了归纳和总结,提出了一种对基于 Web 的网络攻击行为进行分类的方法;Howard 在总结分析了计算机应急处理协调中心 CERT/CC 从 1989 年到 1995 年所收到的事件报告基础上,提出了一种新的攻击分类方法,对攻击的5个属性进行了描述,具体包括攻击者的类型、所使用的工具、入侵过程信息、攻击结果和攻击目的,如图 1.1 所示,Christy 在 Howard 的分类方法基础上对某些项进行了扩充,但基本出发点是一致的;Howard 和 Christy 提出的分类方法易于被大多数人接受,具有较好的实用性,但在一些属性描述细节上存在一些交叉和包含,如图 1.1 和图 1.2中的攻击者和攻击工具中列举的各项。

国内学者在网络攻击分类方面也有一些研究工作:如刘欣然和鲜明等人把目前已有的网络攻击分类方法分为基于经验术语分类方法、基于单一属性的分类方法、基于多属性的分类方法、基于应用的分类方法;祝宁等人针对安全设备和重要主机抗攻击测试的要求,提出了一种基于效果的攻击分类方法,该面向抗攻击测试的攻击分类方式既着眼于攻击对安全设备的作用效果,同时又体现了攻击本身的特征,从而将抗攻击测试建立在用户选择的基础之上,使针对目标设备的抗攻击能力的测试具有了针对性;张涛、董占球在研究国外网络攻击行为分类技术的基础上,

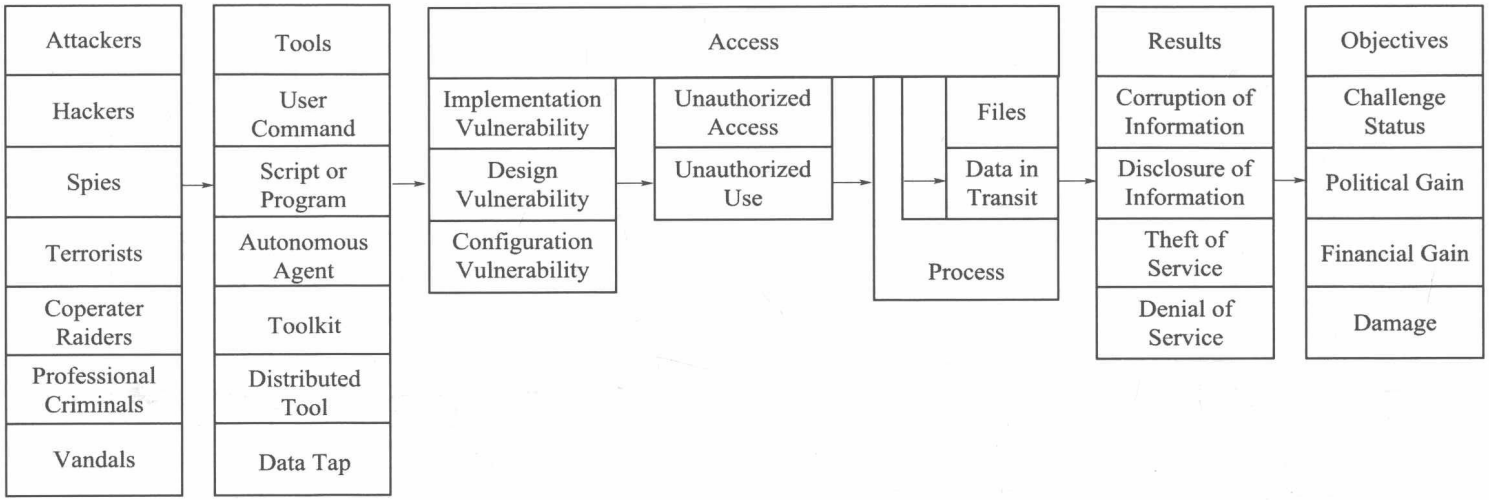

图1.1　Howard提出的攻击分类方法