网络用户行为的安全可信分析与控制

■ 田立勤 著

清华大学出版社　　北京交通大学出版社

网络用户行为的安全可信分析与控制

田立勤 著

内 容 简 介

本书主要论述新型网络中有关用户行为安全可信的分析与控制问题，共10章。第1章主要讲述云计算等新型网络及其对用户行为安全可信需求。第2章主要讲述用户行为信任评估中有关行为证据的预处理问题。第3章主要讲述单次用户行为信任的评估问题，重点讲述了基于层次分析法（AHP）的用户行为信任评估方法。第4章主要讲述长期用户行为信任评估问题，重点讲述了基于滑动窗口的长期行为信任评估机制。第5章主要讲述服务提供者之间如何在共享用户行为信任信息的基础上评估用户行为信任。第6章主要讲述用户行为信任预测问题，重点讲述了基于贝叶斯网络的多条件用户行为信任预测机制。第7、8章主要讲述用户行为的控制问题，包括基于信任预测的用户行为博弈控制机制和基于用户行为信任的动态角色访问控制机制。为了使本书的知识系统完整，第9章讲述了传统的用户身份认证机制，第10章对照传统的用户身份认证机制讲述用户行为认证问题。

图书在版编目(CIP)数据

网络用户行为的安全可信分析与控制/田立勤著. —北京：清华大学出版社；北京交通大学出版社，2011. 8

ISBN 978－7－5121－0701－4

Ⅰ. ①网…　Ⅱ. ①田…　Ⅲ. ①计算机网络－安全技术　Ⅳ. ①TP393. 08

中国版本图书馆 CIP 数据核字(2011)第 170652 号

责任编辑：谭文芳
出版发行：清 华 大 学 出 版 社　邮编：100084　电话：010－62776969
　　北京交通大学出版社　邮编：100044　电话：010－51686414
印 刷 者：北京泽宇印刷有限公司
经　　销：全国新华书店
开　　本：175×245　印张：10. 5　字数：226 千字
版　　次：2011 年 8 月第 1 版　2011 年 8 月第 1 次印刷
书　　号：ISBN 978－7－5121－0701－4/TP·660
印　　数：1～800 册　定价：35. 00 元

前　言

背景

随着诸如云计算、电子金融等新的网络应用的不断出现，传统的基于身份认证的网络安全控制与防护措施已经不能满足网络发展的实际需求（如密码盗号程序盗用了用户密码和被钓鱼网站钓走密码等），迫切需要研究基于用户行为的安全可信与认证的基础理论和研究方法。研究用户行为的安全可信与认证具有如下好处：第一，用户行为可信与认证为从用户源头有效实施网络安全控制提供了重要支撑，具有重大的研究意义和应用价值；第二，用户行为可信与认证是满足诸如云计算等新型网络应用的需求，是对身份认证和内容认证的重要补充；第三，用户行为具有动态多样、随机博弈特性，需要开展专门的工作寻求行为可信与认证的基础理论的创新与应用。

本书主要研究新型网络中有关用户行为安全可信的分析与控制问题。内容包括行为证据的获得与规范化表示，行为认证集的建立，行为认证的机制与模型，行为前的预测，行为中的实时监测与认证，行为后的单次和长期的信任评估与更新，对于不确定的行为认证的风险评估与博弈分析控制，基于行为认证的访问控制等，相对形成一个完整而系统的用户行为的安全可信分析与控制框架。

本书特点与读者对象

本书具有以下鲜明特色。

（1）完整性：内容丰富全面，结构合理，体系完整，对用户行为安全可信的分析与控制进行全面和系统的介绍。

（2）实用性：结合当前网络环境的特点，将网络用户行为可信与认证应用于可信网络和云计算等新型网络应用中，给出具体的应用实例，具有很强的实用性。

（3）学术性：本书具有一定的理论高度和学术价值，书中绝大部分内容取材于作者近期已在国际、国内学术期刊发表的论文，全面展示了大量用户行为安全可信方面最新的科研成果，具有很高的学术参考价值。

本书非常适合我国计算机网络和通信领域的教学、科研和工程应用人员参考。既可以供计算机、通信、电子、信息等相关专业的科研人员、研究生和大学高年级学生作为教材或教学参考书，也可以供计算机网络研究开发人员、网络运营商等网络工程技术人员参考。

致谢

作者的研究工作得到973计划前期研究专项（No. 2011CB311809）、河北省自然科学基金项目（No. F2010001745）和教育部新世纪优秀人才支持计划（NCET－10－0101）的资助，在此表示深深的谢意！

本书的研究工作大都是在我的导师林闯教授的指导下完成的，我现在所取得的成绩离不开他对我的教导和帮助，对此表示衷心的感谢！特别感谢孙锦霞、冀铁果硕士，陈亚睿博士对本书的编写提供的支持和帮助。另外，谭文芳老师在本书的出版过程中做了大量细致辛苦的工作，对此表示衷心的感谢！最后特别感谢青海师范大学提供良好的写作环境和条件，并给予出版费用的资助。

由于作者水平所限，加之用户行为安全可信的研究仍处于不断的发展和变化之中，书中错误和不足之处在所难免，恳请专家、读者指正。

编　者

2011 年 6 月

目　　录

第 1 章　新型网络中的用户行为安全可信需求 …… 1
1.1　可信网络的发展 …… 1
1.1.1　可信网络的提出 …… 1
1.1.2　可信网络的含义 …… 3
1.2　可信网络研究的主要内容 …… 5
1.2.1　服务提供者的可信 …… 5
1.2.2　网络信息传输的可信 …… 6
1.2.3　终端用户的可信 …… 6
1.3　可信网络需要解决的科学问题 …… 6
1.3.1　网络信息传输、服务提供者与用户行为的可信模型 …… 7
1.3.2　可信网络的体系结构 …… 8
1.3.3　服务的可生存性 …… 9
1.3.4　网络的可管理性 …… 10
1.4　可信网络中的可信度量与计算 …… 10
1.4.1　可信度量指标体系 …… 10
1.4.2　可靠性的形式化度量与计算 …… 11
1.4.3　可用性形式化度量与计算 …… 12
1.4.4　可维护性形式化度量与计算 …… 12
1.4.5　故障形式化度量与计算 …… 12
1.4.6　保险性形式化度量与计算 …… 12
1.4.7　可行性形式化度量与计算 …… 13
1.4.8　机密性和完整性形式化度量与计算 …… 13
1.5　可信网络中研究用户行为可信的意义 …… 13
1.6　可信网络中用户行为可信研究的主要内容 …… 14
1.7　云计算的发展 …… 15
1.8　云服务模式与特性 …… 16
1.8.1　云服务模式 …… 16
1.8.2　云服务特性 …… 18
1.9　云计算中服务提供者对用户行为可信的需求 …… 18
1.10　云计算中行为可信的主体分析 …… 19

1.11 用户行为可信的基本准则 …… 21
1.12 用户行为信任的评估、预测与控制整体架构 …… 21
第2章 用户行为信任评估中行为证据的预处理 …… 24
2.1 用户行为信任评估的基本思路与分层分解模型 …… 24
2.2 用户行为证据的定义、分类与获取 …… 26
2.2.1 用户行为证据的定义 …… 26
2.2.2 用户行为证据的分类 …… 26
2.2.3 用户行为信任证据的获取 …… 28
2.3 用户行为信任证据的存储数据结构 …… 29
2.3.1 具有良好可扩展性的信任证据的数据结构 …… 29
2.3.2 基于原始信任证据保留的数据结构 …… 29
2.4 用户行为证据更新 …… 30
2.4.1 用户行为证据更新计算 …… 30
2.4.2 用户行为证据随时间衰减的特性 …… 30
2.5 用户行为证据的规范化表示 …… 31
2.5.1 用户行为证据的常见表示类型 …… 31
2.5.2 用户行为证据表示的差异性分析 …… 31
2.5.3 用户行为证据的规范化表示 …… 32
2.6 用户行为证据的信任化处理 …… 33
2.6.1 用户行为证据信任等级的划分 …… 33
2.6.2 用户行为证据信任等级的确定 …… 35
2.6.3 用户行为证据信任化处理的规则 …… 35
2.6.4 信任化后行为证据的规范化表示 …… 39
2.7 用户行为证据规则库及其查找方法 …… 40
2.8 行为证据预处理的性质分析 …… 45
2.8.1 信任化和规范化预处理后的性质分析 …… 45
2.8.2 信任证据更新预处理后的性质分析 …… 46
第3章 基于 AHP 的分层分解的用户行为信任评估模型 …… 49
3.1 用户行为信任评估的层次分解策略 …… 49
3.2 用户行为信任分层量化评估的基本思路 …… 50
3.2.1 用户行为信任属性的量化评估 …… 50
3.2.2 用户行为信任的量化评估 …… 50
3.3 基于 AHP 的用户行为信任评估 …… 51
3.3.1 AHP 在用户行为信任评估中的作用 …… 51
3.3.2 AHP 的计算方法 …… 51
3.3.3 基于 AHP 的行为信任证据的权重计算方法 …… 53

3.3.4 基于 AHP 的行为信任证据权重的一致性检验 …… 54
3.3.5 基于 AHP 的行为信任属性的权重计算方法 …… 54
3.4 证据不全对信任评估的影响与对策 …… 54
3.4.1 证据获得不全对信任评估的影响 …… 54
3.4.2 不同价值访问的信任属性评估方法 …… 56
3.4.3 不同价值访问的用户行为信任的评估方法 …… 57
3.5 用户行为信任评估的实例与性质分析 …… 58
3.5.1 计算用户安全行为信任属的证据权重 …… 58
3.5.2 用户信任评估中的参数性质 …… 59
第 4 章 基于滑动窗口的用户长期行为信任评估机制 …… 62
4.1 长期用户行为信任评估的原则 …… 62
4.1.1 主观性和客观性的结合 …… 62
4.1.2 用户交往次数的规模性和可扩展性的结合 …… 62
4.1.3 近期行为的重要性和远期行为的衰减性的结合 …… 63
4.1.4 “慢升”与”快降”的结合 …… 63
4.1.5 能保留未信任化的原证据，便于信任的再评估和信任信息共享 …… 63
4.1.6 遵循算法的简单性原则，具有良好的性能和可行性 …… 63
4.2 基于证据更新的长期用户行为信任计算方法 …… 64
4.3 基于滑动窗口的长期行为信任评估机制模型 …… 64
4.3.1 用到的符号说明 …… 64
4.3.2 数据结构 …… 65
4.3.3 信任评估模型定义 …… 66
4.3.4 模型描述 …… 67
4.4 窗口信任记录的更新与信任评估 …… 68
4.4.1 基于新信任触发的窗口信任记录的更新 …… 68
4.4.2 基于过期的窗口信任记录的更新 …… 69
4.4.3 基于不信任的窗口信任记录的更新 …… 69
4.4.4 基于滑动窗口的长期用户行为信任评估 …… 70
4.5 算法的性质分析 …… 72
4.5.1 行为信任评估是主观性和客观性的结合 …… 72
4.5.2 评估是用户交往次数的规模性和可扩展性的结合 …… 72
4.5.3 评估是近期行为的重要性和远期行为的衰减性的结合 …… 73
4.5.4 评估的评估值是“慢升”与“快降”的结合 …… 73
4.5.5 其他信任特性的分析 …… 73
第 5 章 用户行为信任信息的共享、博弈与计算 …… 74
5.1 引言 …… 74

5.2 用户行为信任信息的共享基本结构 …… 74
5.3 用户行为信任信息共享存在的主要问题 …… 75
5.4 基于信誉的信任信息共享博弈模型 …… 76
5.5 基于信誉的信任信息共享模型的纳什均衡 …… 77
5.5.1 纯策略纳什均衡 …… 77
5.5.2 混合策略纳什均衡 …… 78
5.6 基于推荐者类型的用户行为信任计算 …… 79
5.6.1 基于同构推荐者的用户行为信任计算 …… 79
5.6.2 基于非同构推荐者的用户行为信任计算 …… 80
5.6.3 用户行为信任推荐的拓扑结构 …… 81
5.6.4 不同推荐拓扑结构的用户行为信任计算 …… 83
5.7 基于激励机制的推荐者的信任更新计算 …… 85
5.8 基于推荐的用户行为信任计算的性能与特性分析 …… 86
5.8.1 基于博弈论的信任信息共享机制达到整个系统利益最大化 …… 86
5.8.2 具有防止推荐者欺骗的特性 …… 86
5.8.3 计算方法的可扩展性和性能 …… 86
第6章 基于贝叶斯网络的多条件用户行为信任预测模型 …… 88
6.1 用户行为信任预测的意义 …… 88
6.2 用户行为信任的贝叶斯网络模型 …… 88
6.2.1 贝叶斯网络及其理论基础 …… 88
6.2.2 贝叶斯网络的建立及其优点 …… 90
6.2.3 用户行为信任的贝叶斯网络模型 …… 90
6.3 用户行为信任的等级划分和符号说明 …… 91
6.4 用户行为信任的先验概率 …… 92
6.5 用户行为属性的先验概率 …… 92
6.6 结点的条件概率表 …… 92
6.7 用户行为信任的预测 …… 93
6.7.1 用户行为信任预测的整体流程图 …… 93
6.7.2 不同安全要求的用户信任的预测 …… 93
6.7.3 不同性能要求的用户信任的预测 …… 93
6.7.4 不同可靠性要求的用户信任的预测 …… 94
6.7.5 安全和性能任意条件组合的用户信任的预测 …… 94
6.8 行为信任预测的性质分析 …… 95
6.9 应用示例 …… 96
6.9.1 应用示例的背景 …… 96
6.9.2 用户行为信任等级的预测 …… 96

第 7 章　基于信任预测的用户行为博弈控制机制 …… 100
7.1　问题的提出 …… 100
7.2　博弈控制的基本理论 …… 100
7.2.1　博弈论及其要素 …… 100
7.2.2　博弈的分类 …… 101
7.2.3　理性行为 …… 102
7.2.4　策略 …… 102
7.2.5　博弈控制中的纳什均衡 …… 102
7.3　基于用户行为信任预测的博弈控制的整体过程 …… 103
7.4　文中符号说明和双方利益的得失分析 …… 104
7.5　基于用户安全行为信任属性的博弈分析 …… 105
7.6　基于用户行为信任预测的博弈控制策略 …… 107
7.7　应用实例与效果对比分析 …… 108
7.7.1　应用实例的背景 …… 108
7.7.2　应用实例的数据假定与决策计算 …… 109
7.7.3　结果的比较与分析 …… 110
第 8 章　基于用户行为信任的动态角色访问控制机制 …… 111
8.1　问题的提出 …… 111
8.2　TD – RBAC 模型 …… 112
8.3　TD – RBAC 模型的形式化描述 …… 112
8.3.1　各元素形式化描述 …… 113
8.3.2　指派关系描述 …… 114
8.3.3　角色继承描述 …… 115
8.4　TD – RBAC 模型的授权 …… 115
8.5　实时异常行为的监控与防范 …… 116
8.5.1　可实时监控的重要安全属性方面的行为证据 …… 117
8.5.2　基于用户行为信任的异常用户行为的实时监控 …… 117
8.6　模型特性分析 …… 118
8.6.1　TD – RBAC 模型动态性 …… 118
8.6.2　用户行为信任的引入 …… 119
8.6.3　TD – RBAC 模型的角色数量分析 …… 119
8.6.4　TD – RBAC 模型的性能分析 …… 120
8.6.5　实时监控的性能分析 …… 120
8.7　可信网络中用户行为信任控制架构 …… 120
第 9 章　用户身份认证机制 …… 122
9.1　网络安全中用户身份认证概述 …… 122

9.2 用户身份可鉴别性机制的评价标准 …… 123
9.2.1 用户身份可鉴别机制的安全（真实）性 …… 123
9.2.2 身份鉴别因素的数量和种类 …… 123
9.2.3 口令的管理 …… 123
9.2.4 用户身份可鉴别机制是否需要第三方参与 …… 124
9.2.5 是否具备双向身份鉴别功能 …… 124
9.3 用户的网络身份证——数字证书 …… 124
9.3.1 数字证书概述 …… 124
9.3.2 数字证书的内容 …… 124
9.3.3 生成数字证书的参与方 …… 125
9.3.4 证书的生成 …… 126
9.3.5 数字证书的作用 …… 128
9.3.6 数字证书的信任 …… 129
9.3.7 证书吊销 …… 129
9.4 网络安全中用户身份可鉴别性机制与评价 …… 130
9.4.1 基于口令的用户身份鉴别机制与评价 …… 130
9.4.2 基于口令摘要的用户身份鉴别机制与评价 …… 131
9.4.3 基于随机挑战的用户身份鉴别机制与评价 …… 133
9.4.4 基于口令卡的用户身份鉴别机制与评价 …… 136
9.4.5 基于鉴别令牌的用户身份鉴别机制与评价 …… 138
9.4.6 基于数字证书的用户身份鉴别机制与评价 …… 140
9.4.7 基于生物特征的用户身份鉴别机制与评价 …… 141
第 10 章 用户行为认证机制 …… 144
10.1 用户行为认证的必要性 …… 144
10.2 用户行为认证概念与行为证据的获得 …… 145
10.3 用户行为认证集 …… 145
10.4 用户行为认证机制 …… 146
10.5 用户行为认证的评价 …… 149
10.6 行为认证的误报率分析 …… 149
10.7 用户行为认证与控制模型 …… 150
参考文献 …… 153

第 1 章

新型网络中的用户行为安全可信需求

1.1 可信网络的发展

1.1.1 可信网络的提出

网络已发展成为构建和谐社会的一项重要基础设施，它在通信、交通、金融、应急服务、能源调度、电力调度等方面发挥重要作用。网络的规模和应用都在迅速壮大，据《中国互联网发展状况统计报告》[1]显示，截至 2010 年 12 月底，我国网民规模达到 4.57 亿，较 2009 年年底增加 7330 万人；我国手机网民规模达 3.03 亿，依然是拉动中国总体网民规模攀升的主要动力；最引人注目的是，网络购物用户年增长 48.6%，是用户增长最快的应用，这预示着更多的经济活动步入互联网时代。随着网络的发展，网络安全越来越重要。温家宝总理主持召开的国家信息化领导小组第三次会议，也着重强调了保障信息网络安全和促进信息化发展的重要性，并首次将保障信息网络安全作为国家信息化战略的核心内容。事实上，这也是对世界各国积极制定网络空间安全战略的一种反应，如美国《国家计算机空间安全战略》的安全计划就明确地将网络安全提升到了关系国家安全的战略高度。此外还有《日本信息安全技术对策》、《法国信息网络安全管理体系》、《韩国信息通信构建保护法》等。

随着信息通信技术的演进和发展，网络信息安全的内涵不断延伸，从最初的信息保密性发展到信息的完整性、可用性和不可否认性，进而又发展到系统服务的安全性（如身份识别和访问控制等），随后出现多种不同的安全防范机制，例如，防火墙、入侵检测和防病毒等。虽然安全防范的技术不断增多增强，但恶意攻击和恶意程序的破坏却并没有因此而减少和减弱。因此人们只能继续把防火墙、入侵检测、病毒防范做得越来越复杂，但随着维护与管理复杂度的增加，整个信息系统变得更加复杂和难以实施，也使得信息系统的使用效率大大降低，目前分散、独立、单一防御和外在围堵式的网络安全系统已经无法应对具有多样、随机、隐蔽和传播等特点的攻击和破坏

行为，因此网络正面临着严峻的重大安全挑战。

同时，随着网络技术和应用的飞速发展，互联网日益呈现出复杂、异构等特点，当前的网络体系同样暴露出严重的不足，网络正面临着严峻的安全和服务质量（Quanlity of Service，QoS）保证等重大挑战。然而当前的 Internet 是基于 20 世纪 70 年代提出的网络体系结构设计的，随着网络技术的快速发展以及新应用的不断涌现，原先大家普遍接受的网络自由主义理念和管理的无政府状态正在经历着严重挑战，并且不再适应当前实际的网络发展，重新思考网络体系结构已经成为国际研究界的共识，特别是围绕如何保障网络的可信性更是一个研究热点。国际研究表明[2-13]网络安全正向网络可信方向发展，未来网络安全是增加行为可信的可信网络，这也是网络安全研究领域近年来取得的一个新的共识。

正如美国工程院院士 David Patterson 教授所指出：”过去的研究以追求高效行为为目标，而今天计算机系统需要建立高可信的网络服务，可信性必须成为可以衡量和验证的性能。”[14-16]在实现网络安全方面，Rasmusson 和 Jansson[17]首次提出了用硬安全（Hard Security）和软安全（Soft Security）概念来表示两种不同的安全方法。其中，硬安全是通过网络安全技术来保护资源的安全机制，如认证、加密，不可抵赖等；软安全是用类似社会控制机制中的信任和信誉系统来实现网络安全。可见，网络中的最初信任是安全机制的范畴，是实现安全的一种手段。实际上，网络信任不仅是对安全属性的信任，也可以是对性能、收费等各种属性的信任；网络信任不仅可以通过减少或避免与恶意用户的交往来提高网络的安全性，而且由于相互信任提高了服务提供者和用户间合作完成任务的可能性，简化了因不信任带来的监控和防范等额外开销，因此网络信任不仅可以提高网络的安全性而且也可以提高网络的整体性能[18]。

在网络领域里，正式提出以建立“高可信网络”为目标的计划来自中国，旨在以高可信网络满足“高可信”质量水准的应用服务需要。目前“高可信网络”已被正式写进中国国务院公布的《国家中长期科学和技术发展规划纲要（2006—2020 年）》[19]（以下简称《纲要》）。《纲要》明确指出：”以发展高可信网络为重点，开发网络信息安全技术及相关产品，建立信息安全技术保障体系，防范各种信息安全突发事件”。

可信计算只提供了计算机平台的可信，不能提供网络可信，需要进一步将可信扩展到整个网络。1999 年，由 Compaq、HP、IBM、Intel 和 Microsoft 牵头组织了可信计算平台联盟（Trusted Computing Platform Alliance，TCPA）致力于在计算平台体系结构上增强其安全性。2001 年 1 月，TCPA 发布了标准规范；2003 年改组为可信计算集团（Trusted Computing Group，TCG），成员扩大到 200 家。2003 年 10 月发布了可信平台模块（Trusted Platform Module，TPM）规范。2002 年年底 IBM 发布了带有嵌入式安全子系统 ESS 的笔记本电脑，2003 年 月，Intel 推出了 LaGrande 技术。作为可信计算最积极的倡导者，Microsoft 公司宣称将其操作系统建立在“高可信计算”的基

础上。国内目前包括联想在内的8家企业加入了可信计算组。TCG 进一步划分成更详细的研究组，包括体系组，无线移动组，PC 客户机组，服务器组，软件堆栈组，存储组，可信网络连接组，可信平台模块组。可信计算首先检查身份是否可信，例如，它是不是合法的一员，是不是认可的设备等，然后检查用户状态是否可信，例如，它的防御措施是否到位，是否有安全的、合格的防病毒软件，它的终端防病毒软件数据是否及时更新，监督它的防御措施是否到位等。为了提高美国的信息安全和信息信任，美国国家自然科学基金在2006年支持信息空间信任的研究项目，美国国家研究委员会也提出信息空间信任研究建议。我国在可信网络方面也进行了多年的研究，国内也有一些公司已经开始在可信计算终端和网络安全方面开展工作，但较多地处于跟踪国外研究动态的阶段。可信计算列入十一五规划，国家信息中心、北工大等正在进行可信计算终端的研究。清华大学国家信息实验室的网络控制研究组先后在可控可信、可扩展的新一代互联网体系，可信网络，网络安全的随机模型方法与评价技术等相关方面进行了大量的前瞻性的研究。

1.1.2　可信网络的含义

由于可信网络刚刚发展起来，因此业界目前对可信网络有不同理解，下面进行详细论述。

（1）有人认为：可信网络是现有安全技术的整合，即对现有用户网络安全资源的有效整合、管理与监管就是可信网络[20]。

（2）有人认为：可信网络是身份认证的可信。例如，基于公钥基础设施（PKI）的信任链的形成等[21,22]。

（3）有人认为：可信网络是内容可信，即网络传递数据的内容要真实、可信[23,24]。

（4）有人认为：可信网络是网络本身的可信。即网络自身要提供可信的服务能力，保证被传递的数据不能被有意无意篡改和破坏[25]。

（5）有人认为：可信网络是网络服务提供者的可信。例如，提供电子商务的服务提供者提供的服务要可信，不能欺骗用户[26,27]。

（6）有人认为：可信网络是系统平台的可信，如可信计算等[28,29]。

（7）有人认为：可信就是安全，把可信跟安全等价起来[30]。

（8）有人认为：可信网络主要指用户行为的诚信[31]。

（9）也有人把网络软硬件的可靠性和可用性称为可信[32]。

这些不同的理解都是从不同需求和应用角度来阐述网络可信的，因此如何定义一个全面、有效、合理，并能概括这些不同理解的定义才能被大家共同认可，形成合力解决目前网络的疑难问题。

可信网络最初概念是在清华大学林闯教授的”可信网络研究”一文[11]中提出来的，文章在分析可信网络产生的背景和动机的基础上提出了可信网络的概念，揭示了

其基本属性，并讨论了可信网络研究需要解决的关键科学问题。随后清华大学蒋屹新博士的“从可信计算到可信网络”[20]进一步将目前的可信计算如何发展到可信网络进行了论述。我们[33-37]针对可信网络的用户行为信任的评估，预测和控制进行了进一步深入的研究和分析。

我们认为前面对可信网络的不同理解都是相对片面的，真正的可信网络的定义应该是广义的，综合前面各种不同的对可信理解的内容。

***定义 1.1** 可信网络是指网络信息传输、服务提供者和用户的行为及其结果总是可以预期与可管理的。

从定义 1.1 可以看到，可信网络的主体是网络的三个基本组成部分，即网络、服务提供者和用户。可预期是信任的结果，因为可预期是基于信任的，可管理是可以进行控制的，因此可信网络重点强调网络信息传输、服务提供者和用户三者的行为是否可信，是一种动态的行为信任，而不仅仅是传统网络中的静态的身份信任。传统的安全机制被用来提供授权和认证，解决了身份信任的问题，但并不能处理行为的信任问题。例如，在网上钓鱼的例子中，网络本身提供的平台可能是可信的，但由于服务提供者或者用户的行为不可信导致网络的内容不可信。因此行为信任是解决内容安全的根本途径，网络的各种表现最终归结为网络信息传输、服务提供者和用户的行为所致。同时动态的行为信任可以提供比身份信任更细粒度的安全保障。

总之，可信网络要能够做到：行为状态可监测，行为结果可评估，异常行为可管理。具体而言，网络的可信性应该包括一组属性，从用户的角度需要保障服务的安全性和可生存性，从设计的角度则需要提供网络的可管理性。

下面根据定义 1.1，分析业界对可信网络的不同理解与本书定义的可信网络的关系。

可信网络没有抛弃理解（1）中的现有网络的安全技术，而是在现有安全技术上增加对网络，服务提供者和用户行为信任的动态评估，预测与管理，这些行为信任评估，预测与管理的安全离不开传统的加密，身份认证，访问控制等技术的配合，因此理解（1）是包含在定义 1.1 中的。

理解（2）是可信网络中隐含的内容，我们要对网络、服务提供者和用户进行行为信任的评估，预测与管理就必须首先确定其身份，因此身份可信任是行为可信任的前提和基础，但身份信任并不等于行为信任。例如在数字化电子资源的订购方面，大学生通过可信的身份信任（一般是学校的 IP 地址）可以登录到学校订购的数字资源服务器上，但他的行为却有可能是不可信的，如利用下载工具大量下载文章，私设代理服务器等不可信行为来谋求自己的利益。因此理解（2）是包含在定义 1.1 中的。

理解（3）和（8）是指参与网络的服务提供者和用户行为要可信，因为只有这样才能达到内容可信和行为诚心，它是可信网络中三个主要主体中的其中两个。因此理解（3）和（8）是包含在定义 1.1 中的。

理解（4）和（6）都是指网络的信息传输要可信，是可信网络中三个主要强调的内容之一，因此理解（4）和（6）是包含在定义 1.1 中的。

理解（5）是指服务提供者的行为要可信，它是可信网络中三个主要强调的内容之一，因此理解（5）是包含在定义 1.1 中的。

理解（7）是对可信网络的片面理解，因为可信网络不仅是指传统网络安全方面的可信，还可以包括服务提供者和用户的诚信。本书所指的用户行为信任还包括用户的性能和可靠性等方面的信任，因为用户的性能和可靠性方面的信任直接影响服务提供者提供的服务好坏。例如，在数字化电子资源的订购方面，用户下载文章的速率，用户的对服务器的响应时间等属于性能方面的行为信任，这些性能方面的行为信任对于充分利用用户连接数有限的数据资源来说具有重要的意义，因为下载同样多的数据，性能方面行为信任低的用户将占用服务的时间长，其他的用户就可能因为用户连接数满而得不到服务，因此不能将可信网络仅仅等价与安全网络。因此理解（7）是包含在定义 1.1 中的。

理解（9）也是对可信网络的片面理解，因为可信网络不仅是指网络软硬件的可靠性，可靠性只是可信网络多个信任方面的一个，评估、预测和管理网络软硬件的可靠性是保证可信网络中网络信息传输可信的一个重要内容之一，因此理解（9）也是包含在定义 1.1 中的。

1.2　可信网络研究的主要内容

网络可信是在原有网络安全技术的基础上增加行为可信的安全新思想，强化了对网络状态的动态处理，为实施智能自适应的网络安全和服务质量控制提供策略基础。网络可信包括三个方面的内容：服务提供者的可信、网络信息传输的可信和终端用户的可信。

1.2.1　服务提供者的可信

服务提供者可信又包括两个方面的内容，包括服务提供者的身份可信和行为可信。服务提供者身份可信是指服务提供者的身份可以被准确鉴定，不被他人冒充，即服务提供者的身份真实有效。服务提供者行为可信是指判断服务提供者的行为是否真实可靠，不带有欺骗性，对用户终端是否会带来安全危险等。

传统的安全机制可以解决服务提供者的身份信任问题，但并不能处理服务提供者的行为信任问题。服务提供者的行为信任包括两个方面，即基本行为信任和高级行为信任。基本行为信任是指服务提供者的行为是否真实可靠，不欺骗、不随意中断服务，是否按契约的规定提供服务等。例如，在学校的数字资源的使用方面，服务提供者是否按规定及时提供可靠的数字资源，提供的内容与规定的契约相符合，不虚假、不欺骗，并随时可用等。高级要求是指服务提供者在提供服务的行为过程中是否对给

用户的安全带来破坏行为，包括提供的内容是否带有恶意程序，是否将用户的私有信息透漏给第三方，是否为了商业利益对用户进行了其他的破坏行为等。例如，在学校的数字资源的使用方面，服务提供者内容是否携带病毒、蠕虫和木马等可能影响用户安全的恶意程序，是否将用户的私有信息，如电子邮件等有意无意透漏给第三方，使得用户不断收到垃圾邮件从而给用户留下安全隐患，以及是否将不安全的超级链接通过服务提供者的页面提供给用户等。

1.2.2 网络信息传输的可信

网络信息传输的可信性是指网络各结点在传输信息的过程中是否忠实，不删、不改、不夹带。在传输信息时可以根据用户的要求在指定的路径上传输信息，其核心是保证信息在传输过程的保密性、完整性和可用性。网络信息传输的可信性一方面要防止第三方对网路传输信息的破坏，另一方面也要防止网络本身可能给传输的信息带来破坏。在制定的策略方面，一方面要在接收方和发送方从技术上保证传输信息的可信性，另一方面也要从法律制度、管理和技术等方面保证网络信息不被网络本身和第三方破坏的可信性。

1.2.3 终端用户的可信

终端用户可信也包括两个方面的内容：终端用户的身份和行为可信。终端用户身份可信是指终端用户的身份可以被准确鉴定，不被他人冒充，即终端用户的身份真实有效。终端用户的行为可信是指终端用户的行为是否可以评估、可预期、可管理、对网络设备和数据是否会造成破坏或毁坏。

传统的安全机制可以解决用户的身份信任问题，但并不能处理用户的行为信任问题。例如在数字化电子资源的订购方面，大学生通过可信的身份信任（一般是学校的 IP 地址）可以登录到学校订购的数字资源服务器上，但他的行为却有可能是不可信的。例如，一些学生在校内（身份信任是合法的）常常使用网络下载工具大批量下载学校购买的电子资源或者私设代理服务器牟取非法所得等，即用户的身份信任是可信的，但用户的行为信任不一定是可信的。

1.3 可信网络需要解决的科学问题

可信网络的研究将面临四个重要的科学挑战：第一，由于网络攻击、破坏行为的多样性、随机性、隐蔽性和传播性，使用现有的网络模型理论已经难以实现对其进行描述分析；第二，网络尤其是互联网络的体系结构中，“边缘论”和面向非连接的设计思想保障了高效的互通，但控制手段相对薄弱，难以满足解决现实网络安全问题的需要；第三，网络固有的脆弱性，人为的操作失误和管理漏洞，以及网络攻击和破坏