网络信息内容审计

孙钦东等　编著

電子工業出版社
PUBLISHING HOUSE OF ELECTRONICS INDUSTRY
http://www.phei.com.cn

网络信息内容审计

孙钦东　李胜磊　李庆海　黄新波　编著

電子工業出版社
Publishing House of Electronics Industry
北京·BEIJING

内 容 介 绍

网络信息内容审计是一门对网络中传输的信息内容进行分析的技术，是网络安全技术中不可或缺的重要组成部分，通过内容审计可实现网络信息内容的可控性。本书按照从整体到局部的思路，以从底层到高层的视角，详细分析了内容审计所涉及的主要技术的原理与实现，并探索了一些关键技术和共性问题。同时，对当前日益严重的手机短信内容安全问题进行了讨论。

本书是进行信息内容分析与识别方面的参考书，可作为从事网络信息内容安全、网络舆情分析与预警等研究领域科研人员的参考书，也可作为高等院校网络安全专业大学生与研究生的参考教材。

图书在版编目（CIP）数据

网络信息内容审计 / 孙钦东等编著.—北京：电子工业出版社，2010.1
ISBN 978-7-121-09649-5

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

中国版本图书馆 CIP 数据核字（2010）第 180108 号

责任编辑：毕军志　文字编辑：裴杰
印　　刷：北京市天竺颖华印刷厂
装　　订：三河市鑫金马印装有限公司
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
开　　本：720×1000　1/16　印张：18.5　字数：480 千字
印　　次：2010 年 1 月第 1 次印刷
印　　数：2000 册
定　　价：39.00 元

凡所购买电子工业出版社图书有缺损问题，请向购买书店调换。若书店售缺，请与本社发行部联系，联系及邮购电话：（010）88254888。

质量投诉请发邮件至 zlts@phei.com.cn，盗版侵权举报请发邮件至 dbqq@phei.com.cn。

服务热线：（010）88258888。

前　言

网络信息内容审计针对网络流量中不良信息传播的问题，从网络中的关键点收集数据包，综合运用网络数据包获取、信息处理、不良流量阻断等技术，对其所传送的内容进行审计分析，实现对网络信息内容的可控性，是网络安全中不可或缺的重要组成部分。伴随着计算机网络的飞速发展，网络信息内容审计在系统模型、核心匹配算法、信息传播机制及审计技术等方面，需要进行深入的研究。

作者在网络信息及手机短信息内容审计方面开展了较长时间的研究，在系统模型、匹配算法、信息扩散机制等多个方面进行了深入的研究，试图按照从整体到局部的思路，以从底层到高层的视角对内容审计所涉及的关键技术进行研究与论述，为内容审计相关技术研究提供参考。书中详细分析了内容审计所涉及的主要技术的原理与实现，探索一些关键技术和共性问题。同时，讨论了手机短信的内容安全问题。

全书共分 11 章。第 1 章介绍了网络信息内容审计的发展现状及相关问题；第 2 章介绍了网络信息内容审计的系统模型；第 3 章讨论了内容审计数据包的获取技术；第 4 章介绍了内容审计中的模式匹配算法；第 5 章介绍了内容审计中的文本分类问题；第 6 章介绍了电子邮件内容的审计；第 7 章介绍了网络不良多媒体信息内容的审计；第 8 章介绍了手机短信内容的审计；第 9 章介绍了手机短信通信网络的演化模型；第 10 章介绍了审计系统的自身安全问题；第 11 章讨论了当前内容审计研究中的热点与难点问题。

本书是进行信息内容分析与识别方面的参考书，可作为从事网络信息内容安全、网络舆情分析与预警等研究领域科研人员的参考书，也可作为高等院校网络与信息安全专业大学生与研究生的参考教材。

参与本书编写的人员有孙钦东、李胜磊、李庆海、黄新波、王倩、郭晓军

等。其中，孙钦东撰写了第 1 章、第 2 章、第 3 章中的 3.1、3.2 和 3.3 节，第 4 章中的 4.1、4.2、4.3 和 4.5 节，第 5 章，第 7 章、第 8 章、第 9 章、第 10 章和第 11 章；李胜磊撰写了第 3 章中的 3.6 节，李庆海撰写了第 6 章中的 6.1 节和 6.2 节，黄新波撰写了第 4 章中的 4.4 和 4.6 节，王倩撰写了第 6 章中的 6.3 和 6.4 节；郭晓军撰写了第 3 章中的 3.4 和 3.5 节。孙钦东对全书进行了统稿。此外，任杰、王楠、何少鹏、李颖洁、刘宝忠、张嵘、马哲等参与了本书的校对工作。

在本书完稿之际，作者衷心感谢电子工业出版社董亚峰老师的大力支持，衷心感谢国家自然科学基金的资助（No. 60802056）。

网络信息内容审计涉及技术众多，发展也十分迅速，由于作者知识水平所限，书中疏漏与欠妥之处在所难免，恳请读者批评指正。

编著者

2009 年 8 月于西安

目　录

第1章 绪 论

进入 21 世纪以来，互联网和移动通信网络的普及浪潮已席卷世界每个角落，对人们工作、学习、生活等都产生了非常深刻的影响。然而，这些通信网络在带来丰富信息的同时，自身安全形势日益严峻。网络病毒肆虐、黑客入侵破坏、非法信息泛滥、谣言短信传播等各种网络安全相关事件频繁发生。其中，由色情、暴力、诈骗、谣言、恶意骚扰等各种不良信息无监督传播而引发的网络信息内容安全问题尤为突出。

如何加强网络信息安全管理，保证网络信息内容的合法性、健康性和安全性，已成为网络通信领域亟待解决的重大问题。在此情况下，网络信息内容审计应运而生，为应对网络信息内容安全问题提供了有效对策。目前，网络信息安全审计作为一种有效的管理措施和取证手段已经被许多国家所接受，并得到多数公众的认可，成为保证网络安全不可或缺的重要组成部分，其相关理论技术研究也越来越得到人们的重视。

本章将简要讨论网络安全和网络信息内容安全的相关概念，介绍网络信息内容审计研究的发展情况，描述网络信息内容审计系统通常具有的功能。

1.1 网络安全与网络信息内容安全

网络安全是指通过采用各种技术和管理措施，保护网络系统中所有软件、硬件、信息等资源免受偶然或恶意的破坏、篡改和泄露，确保网络数据的完整性、保密性、可用性、可控性和不可否认性，以保证各种网络服务正常运行。

从广义上说，网络安全包括网络硬件资源和信息资源的安全性。硬件资源包括通信线路、通信设备（交换机、路由器等）、主机等，是实现信息快

速、安全地交换的必要条件；信息资源包括维持网络服务运行的系统软件和应用软件，以及在网络中存储和传输的用户信息数据等。通常，网络安全具有以下基本特征[1]。

（1）完整性。完整性是指数据在未经授权的情况下不能被更改的特性，即信息在存储或传输过程中保持不被修改、不被破坏和丢失的特性。数据完整性的目的就是保证计算机系统上的数据和信息处于一种完整和未受损害的原始状态。

（2）保密性。保密性是指信息不泄露给非授权的用户、实体或过程，或防止非法用户利用的特性，包括信息的网络传输保密性和存储保密性。数据保密性就是保证具有授权用户可以访问数据，而限制其他人对数据的访问。

（3）可用性。可用性是指被授权实体能够访问并按需求使用与自己权限相对应信息的特性，即能否存取和访问所需的信息。

（4）不可否认性。不可否认性是指在信息交互过程中，保证参与者身份、参与者所提供信息的真实同一性，即所有参与者对本人在通信过程中的身份、所提供的信息，以及所完成的操作与承诺等均不能否认或抵赖。

（5）可控性。可控性是指对信息的内容及传播具有控制能力，即按既定的安全规则、安全策略等实现对信息有效的识别、阻断和监管。

为了满足上述网络安全的基本特征，必须从以下几个方面保证安全：网络中运行系统的安全，即保证信息处理和传输系统的安全，侧重于保证系统的正常运行，避免因系统崩溃、损坏而对系统存储、处理和传输的信息造成破坏、损失；网络上系统信息的安全，包括用户口令认证，用户存取权限控制，数据加密等；网络上信息的安全，侧重于保护信息的保密性、真实性和完整性，避免攻击者利用系统的安全漏洞进行窃听、冒充、诈骗等有损于合法用户的行为；网络上信息传播的安全，侧重于防止和控制非法、不健康信息的传播，避免网络上大量不良信息的传输失控。

从上面叙述可以看出，网络安全的目标实质就是保证网络服务的可用性和有效性，据此网络安全也可以划分为网络功能安全和网络内容安全两个层次，如图 1-1 所示。

第一层为网络功能安全，要求网络能够向用户提供可靠的网络服务和完整有效的信息资源，包括访问控制（Access Control）、身份认证（Authenticity）、数据完整性（Integrality）、数据机密性（Privacy）、抗否认（Non-repudiation）等。保障网络功能安全的技术主要有防火墙（Firewall）、虚拟专用网（Virtual

Private Network，VPN）及入侵检测系统（Intrusion Detection System，IDS）等。

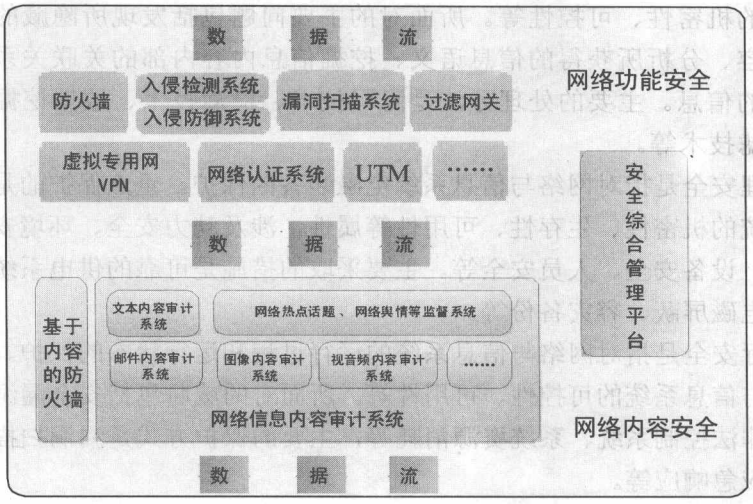

图 1-1　网络安全框架

第二层为网络内容安全，在网络服务可用的前提下，保证网络中传送数据的内容性质符合既定的安全策略，避免数据遭到滥用，保障传输内容的安全性。这方面的技术主要包括基于内容的防火墙和网络信息内容审计系统。两者之间既有相同之处，如都要依赖模式识别技术进行非法、敏感信息的过滤；也存在一定差异，如前者通常丢弃那些被判别为违反安全策略的数据包，后者则给出相应的报警并保存证据。

另外，也有学者给出了其他的网络信息安全层次框架[2]，如图 1-2 所示。该框架给出了网络信息安全层次的概念，描述了各层次的职责和重点保护内容，并给出了应采取的主要技术手段。

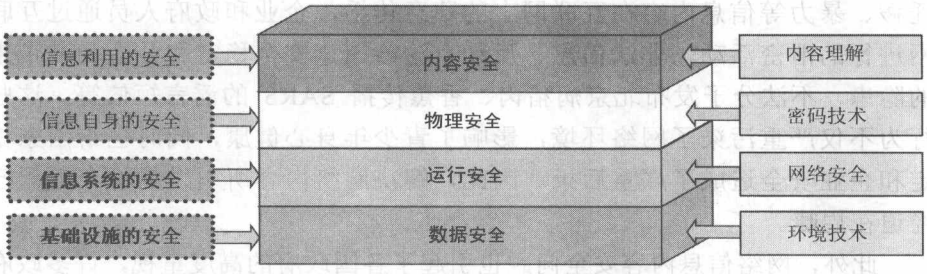

图 1-2　网络信息安全层次框架

内容安全是指对信息真实内容的隐藏、发现、分析以及阻断。主要涉及信息的机密性、可控性等。所面对的主要问题包括发现所隐藏的信息的真实内容、分析所获得的信息语义、挖掘信息内容内部的关联关系、阻断所指定的信息。主要的处理方法是隐写技术、检索技术、数据挖掘技术、信息过滤技术等。

物理安全是指对网络与信息系统电磁装备的保护。重点保护的是网络与信息系统的机密性、生存性、可用性等属性，涉及动力安全、环境安全、电磁安全、设备安全、人员安全等。主要采取的措施是可靠的供电系统、防护体系、电磁屏蔽、容灾备份等。

运行安全是指对网络与信息系统的运行过程和运行状态的保护。主要涉及网络与信息系统的可控性、可用性等。所面对的威胁包括安全漏洞的恶意利用、非法控制系统、系统资源消耗等，主要的保护方式是漏洞扫描、入侵检测、应急响应等。

数据安全是指对信息在数据处理、存储、传输、显示等过程中的保护，使得在数据处理层面信息依据授权而使用，保障不被冒充、窃取、篡改、抵赖。主要涉及信息的真实性、机密性、完整性、不可抵赖性等。主要的保护方式有认证、加密、完整性验证、数字签名等。

上述两个框架模型从不同角度对网络安全的含义进行了较为完整的阐述。可以看出，网络安全的目的不仅要保证网络信息物理上的安全传递，而且还要对网络信息内容进行理解，确保所传播的网络信息内容的合法性、可控性等。因此，充分保证网络信息内容的安全，对实现真正意义的网络安全是至关重要的。

近年来随着 Internet、移动通信网络在国内的迅猛发展[3, 4]，这两者所面临的网络信息安全问题也变得十分突出。各种非法网络行为层出不穷，如淫秽、暴力等信息内容在互联网上的肆意传播，企业和政府人员通过互联网进行的泄密活动，非法信息、反动言论给国家安全稳定和社会和谐带来的隐患，不法分子发布北京病猪肉、香蕉传播 SARS 的谣言短信等。这些行为不仅严重污染了网络环境，影响了青少年身心健康，同时也给国家稳定和企业安全造成了严重后果。因此，解决网络内容所引发的安全问题已经迫在眉睫。

此外，网络信息内容安全问题也引起了各国政府的高度重视，许多政府都出台了相关法律，对网络上的信息内容进行规范和控制。例如，1996 年英国颁布《三 R 互联网安全规则》，旨在消除网络上的儿童色情内容和其他有

害信息；1998年美国通过《儿童在线保护法》对网络信息的内容合法性做出了规定，同时还制定《信息自由法》、《电子通信隐私法》等法规加强对网络言论的规范和保护；1996年德国出台《信息和通讯服务规范法》，对《刑法典》、《治安法》、《传播危害青少年文字法》进行相应的修改和补充。我国政府针对网络信息内容的管理，也制订了相关的法律法规。例如，1997年12月颁布了《计算机信息网络国际联网安全保护管理办法》，2000年9月颁布了《互联网信息服务管理办法》等多个涉及互联网信息的法律文件，都对非法的网络信息内容做出了明确的规定。

综上所述，无论是对于Internet，还是移动通信网络，仅仅保证网络的畅通、网络节点的安全已远远不能够满足当前形势对网络安全的需求，如何保证网络信息内容的合法性、健康性已成为网络安全研究领域中亟待解决的重大问题，针对网络信息内容安全的相关技术研究也已引起各国学者越来越多的关注。其中，网络信息内容审计系统及其相关技术就是研究热点之一。

网络信息内容审计是指通过采取一定的技术手段，监管网络中不良文本、图片、视频等各类信息的传播行为，以保证网络所传播的各类信息内容的健康性、合法性，提供干净的网络信息环境。它侧重于理解网络所传播的信息内容，判断信息内容的性质，并根据相关的安全策略，对非法、不良等各类网络信息进行有效控制和管理，是网络安全中保障信息资源安全性的重要组成部分。

1.2 网络信息内容审计研究概况

网络信息内容审计综合运用信息过滤、信息检索、自然语言处理、图像处理、视音频处理、人工智能等领域的技术对网络所传输的各类信息进行审计检测，监控网络中非法、不良信息的传播，为净化网络环境提供有效保障。网络信息内容审计涉及多项信息处理相关技术，其发展也随信息处理技术的发展而前进。

在国外，与信息处理相关的研究开展时间较长，取得了一定研究成果，主要体现在信息检索、信息过滤等方面。1982年，在电子邮件开始出现之时，美国学者Denning指出以往的信息管理着重于信息的处理与分发，信息的控制和过滤同样需要引起注意，并提出信息过滤（Information Filtering）的概

念[5]。Belkin 详细阐述了信息过滤与信息检索之间的区别与关联[6]。1991 年，在美国新泽西州召开的高性能信息过滤会议讨论了不同的过滤方法、高速过滤系统结构及不同的过滤软件原理等[7-9]，在信息过滤方面进行了初步的研究。1992 年，美国国家标准和技术研究所（National Institute of Standards and Technology，NIST）与 DARPA 联合支持了每年一次的文本检索会议（Text Retrieval Conference，TREC），对文本检索和文本过滤的发展起到了极大的促进作用。TREC 最近的几次会议都着重于文本过滤的理论和技术研究，以及系统测试评价，对信息过滤技术的发展与完善提供了强有力的支持[10-13]。Minnesota 州立大学计算机科学与工程系设立了 Grouplen 项目，该项目包括了同级信息过滤、合作过滤、推荐系统、自动过滤等内容[14,15]。1996 年，该系开发了新闻组（Usenet）过滤软件，后来又开发了 Movielen 多媒体视频推荐系统。另外，Minnesota 州立大学计算机系的 Robert Cooley 等人开发了 Web 站点信息过滤系统 WebSIFS（Web Site Information Filter System）[16]，该系统使用站点的内容和结构信息来自动生成信念集，利用信念集确定潜在兴趣。1993 年，马里兰大学设立了信息过滤项目，由电子工程系的医学信息和计算机认知实验室进行网络信息的过滤研究与实验。1995 年，美国一些图书馆联合实施一项网络信息过滤计划（InfoFilter Project），其目的是制定一套对网络信息进行评价与选择的标准。1998 年，在瑞典召开的机器学习与信息过滤学术研讨会认为网络信息的过滤是进行信息管理的一个重要环节[17]。Borges 被认为是第一个真正实行网络信息过滤的系统[18]。2000～2006 年，随着图像处理技术的发展，关于网络不良信息图像识别也有了一定的研究进展，出现了多种不同的识别方法，如肤色纹理特征方法[19-21]、形状特征方法[22]、分类法（神经网络、SVM）[23-26]等。这些研究工作都为网络信息内容审计奠定了良好的基础。

与学术方面研究相对应，国外的多家网络安全及防病毒公司在网络信息内容安全方面也掌握了一定的技术，能够提供较完整的企业网络内容安全解决方案，如 Symantec 公司提供了 Web 内容过滤器 I-Gear 和 E-mail 过滤器 Mail-Gear，Trend Nucro 以插件的形式提供 Manager 系列的电子邮件安全管理系统和 Web 安全管理系统，SurfControl 美讯智公司提供的内容安全产品包括网页过滤器、邮件安全信息网关（具备防病毒和防垃圾邮件功能）、即时信息过滤器等。同时还产生了多个知名的商业或学术方面的搜索引擎站点，如 Google 等。

与国外研究相比，国内在网络信息内容安全方面的研究起步较晚，在