信息安全技术丛书

门级信息流分析理论及应用

胡 伟 慕德俊 著

科学出版社

信息安全技术丛书

门级信息流分析理论及应用

胡 伟 慕德俊 著

科学出版社
北京

内 容 简 介

本书详细论述了门级信息流跟踪方法的基础理论与应用。首先介绍该方法的基本原理，包括门级信息流跟踪逻辑的性质定理、形式化描述、生成算法与复杂度理论、设计优化问题；然后介绍该方法的应用原理、设计方法学、设计与验证环境，以及该方法在开关电路设计等相关领域的应用等内容，并提出了一些供参考的研究方向。

本书可供信息安全、计算机体系架构和电子设计自动化领域的广大科研工作者、教师和研究生阅读。

图书在版编目(CIP)数据

门级信息流分析理论及应用/胡伟，慕德俊著. —北京：科学出版社，2014.11

（信息安全技术丛书）

ISBN 978-7-03-042370-2

Ⅰ. ①门… Ⅱ. ①胡… ②慕… Ⅲ. ①信息安全 Ⅳ. ①TP309

中国版本图书馆 CIP 数据核字（2014）第 257157 号

策划编辑：陈 静 / 责任编辑：陈 静 邢宝钦 / 责任校对：胡小洁

责任印制：张 倩 / 封面设计：迷底书装

科学出版社 出版

北京东黄城根北街 16 号

邮政编码：100717

http://www.sciencep.com

文林印务有限公司 印刷

科学出版社发行 各地新华书店经销

*

2014 年 11 月第 一 版 开本：720×1 000 1/16

2014 年 11 月第一次印刷 印张：14

字数：280 000

定价：72.00 元

（如有印装质量问题，我社负责调换）

作 者 简 介

胡伟，男，1982 年 10 月生，分别于 2005 年、2008 年和 2012 年获得西北工业大学“信息对抗技术”专业学士、“模式识别与智能系统”专业硕士和“控制科学与工程”专业博士学位，2009 年 9 月—2011 年 9 月赴加州大学圣迭戈分校计算机科学与工程系学习，2012 年 7 月入西北工业大学“计算机科学与技术”博士后流动站，主要从事硬件安全、高可靠系统安全、嵌入式安全、可重构计算等方面的研究。

慕德俊，男，1963 年 6 月生，西北工业大学自动化学院教授、博士生导师，主要研究方向包括网络与信息安全、控制理论与应用、网络化控制、无线传感器网络等。

前　言

用于军用武器、工业基础设施、通信网络和生物医疗等领域的高可靠系统都对信息安全有严格的要求。然而，随着物联网(Internet of things)、信息物理系统(Cyber Physical System，CPS)、云计算(cloud computing)等领域的兴起，高可靠系统面临着前所未有的网络安全(cyber security)威胁，其中尤以物理系统信息安全问题最为突出。近年来，高可靠系统信息安全事件频频发生。2010 年 9 月和 2011 年 4 月，伊朗核电站连续两次发生针对工业控制设备的震网病毒(stuxnet)攻击事件；2011 年 11 月，美国伊利诺伊州 Curran-Gardner 城区供水设施的监控与数据采集(Supervisory Control and Data Acquisition，SCADA)系统遭到网络攻击，最终导致水泵烧毁；2011 年 12 月，美国 RQ-170 无人侦察机因为受到干扰被俘获。另据相关文献报道：黑客可通过无线信道对汽车内部网络、心脏起搏器、胰岛素泵等关键安全设备实施攻击，并能够远程控制这些设备的运行状态。此外，智能电网等关键基础设施也正面临着前所未有的安全挑战。大量安全事件表明：高可靠系统信息安全问题日益突出，并亟待解决。

鉴于上述安全问题与传统信息安全问题在攻击对象和途径上的根本差异，学术界兴起了研究信息物理安全问题的热潮，期望能够从硬件底层为系统构建一个可信、可靠、可验证的安全基础，并为解决上层应用的安全问题提供一种关键安全属性的度量、控制和验证能力，其重点研究方向包括以下几个方面。

(1)安全属性的度量与形式化验证。采用形式化的方法和手段对系统的安全属性(如机密性和完整性)进行度量，为系统关键安全属性的形式化验证提供支撑。

(2)可信安全基础的构建。从硬件底层为系统构建一个可信、可靠、可验证的安全基础，保障系统的可信计算环境不会受到干扰，敏感信息不会发生泄露。

(3)上层应用安全属性的测试与验证。基于底层硬件架构所提供的安全属性度量、控制与验证能力实现上层应用关键安全属性的测试与验证，以及软硬件安全联合验证。

本书在前人的研究基础上，从信息流安全角度探讨高可靠系统的信息安全问题，重点阐述了门级信息流跟踪方法的基础理论与应用，主要包括该方法的基本原理、门级信息流跟踪逻辑的性质定理、形式化描述、生成算法、复杂度理论、设计优化方法、门级信息流跟踪方法的应用原理等。全书共包括 10 章和附录，由胡伟、慕德俊、张慧翔、杨涛、张德刚撰写。本书的主要内容包括以下几个方面。

(1)二级安全格(LOW⊏HIGH)下的门级信息流跟踪理论。介绍了门级信息流

跟踪方法的基本原理，提出并证明了门级信息流跟踪逻辑的若干基本性质，并对基本逻辑单元的信息流跟踪逻辑进行了形式化描述。

(2)多级安全格下的门级信息流跟踪方法。将门级信息流跟踪方法扩展至多级安全格(multilevel security lattice)，并给出了一种保证高可靠系统多级安全(Multilevel Security，MLS)需求的途径。

(3)“精确门级信息流跟踪逻辑生成”问题。证明了该问题的NP完全性，提出了多种门级信息流跟踪逻辑生成算法，包括暴力算法、0-1算法、构造算法、完全和算法、SOP-POS算法、BDD-MUX算法，以及扇出重回聚区域重构算法，并对所提出算法的复杂度进行了分析证明。

(4)门级信息流跟踪方法的应用。讨论了门级信息流跟踪逻辑的设计优化问题，以及门级信息流跟踪方法的应用原理，并结合设计实例介绍了该方法在软硬件安全测试与验证中的应用。

期望本书的出版能起到抛砖引玉的作用，促进相关领域的科研工作者密切关注高可靠系统的信息安全问题，并对其进行深入的研究。

本书的出版得到国家自然科学基金(61303224)、教育部博士点基金(20126102110036)和中国博士后科学基金面上项目(2013M532081)的资助，在此深表谢意；感谢加州大学圣迭戈分校(University of California，San Diego)的Kastner教授、加州大学圣巴巴拉分校(University of California，Santa Barbara)的Sherwood教授和西北工业大学的戴冠中教授，他们在本书的研究工作过程中提出了许多宝贵的指导意见；感谢西北工业大学的毛保磊、郜瑜、郭蓝天等博士研究生，他们在本书的写作过程中做了大量的辅助工作。

作　者

于西北工业大学

2014年4月

目　录

第1章 绪 论

信息安全问题由来已久，已广泛渗透于政治、经济、军事、社会生活等各个领域。本章主要探讨信息安全问题在不同发展阶段下的主要体现形式和未来的发展趋势，重点讨论在物联网、信息物理系统、云计算等领域不断兴起的技术背景下，高可靠系统所面临的网络安全威胁，以及密码算法、认证和访问控制(Access Control，AC)等典型安全机制在应对这些新型安全威胁方面所存在的不足。

1.1 信息安全问题的起源与发展

1.1.1 信息安全问题的起源

回顾信息安全学科的发展历程，我们发现早在人们意识到信息安全问题的重要性之前，就已经有了信息安全的应用需求和案例。远在古希腊时期，人们就已经采用简单的隐写术来传递情报，后来保密通信的需求又促生了一些经典密码算法，如恺撒密码、维吉尼亚密码、移位式密码和莫尔斯码等[1]。但在计算机和网络诞生之前，人们还没有将信息安全作为一个概念或问题正式提出。

2005 年 Whitman 和 Mattord 认为信息安全起源于计算机安全。自从第二次世界大战期间开发出第一代用于帮助分段计算代码的大型计算机以来，计算机安全的需求就诞生了。据查证，“计算机安全”概念是 1969 年提出的，当时美国兰德公司给美国国防部的报告中指出“计算机太脆弱了，有安全问题”[2]——这是首次公开提到计算机安全。

1.1.2 信息安全问题的发展历程

信息安全在其发展过程中主要经历了以下三个阶段。

(1)早在 20 世纪初期，通信技术尚不发达，面对电话、电报、传真等信息交换过程中存在的安全问题，人们强调的主要是信息的机密性，对安全理论和技术的研究也仅侧重于密码学，这一阶段的信息安全可以简单称为通信安全(Communication Security，COMSEC)。

(2)20 世纪 60 年代后，半导体和集成电路技术的飞速发展推动了计算机软硬件的发展，计算机和网络技术的应用进入了实用化和规模化阶段，人们对安全的关注已经逐渐发展为以机密性、完整性和可用性为目标的信息安全(Information

Security，INFOSEC)阶段。

(3)从20世纪80年代开始，由于互联网技术的迅猛发展，信息无论对内还是对外都得到极大开放，由此产生的信息安全问题跨越了时间和空间，信息安全的焦点已经不仅是传统的机密性、完整性和可用性三个原则，由此衍生出如可控性、抗抵赖性、真实性等其他的原则和目标，信息安全也转化为从整体角度考虑其体系建设的信息保障(Information Assurance，IA)阶段。

“9·11”事件以后，不只是美国，世界各国都有意识地增加了对信息技术的投入和监管，可以说“9·11”事件是美国乃至全世界信息安全政策的分水岭。美军参谋机构发行的《2010年联战远景》白皮书为信息战做了如下注释：“鉴于现代计算机网络、通信系统及电子数据库重要性的日益提升，将信息安全纳入国家整体安全政策中仍属必要。在平时，信息战有助于预防冲突发生，或应对危机及公开敌意行为。在危险爆发时，信息战可以用来解决纷争、增强吓阻，或准备应对公开冲突。在战时，信息战则可以直接达成战略、作战及战术目标，或强化其他用于达成这些目标的方法。”可见，信息安全问题在未来很长一段时间内，都将处于非常高的战略高度。

2005年，国际电信联盟以物联网为主题的年度互联网报告大力推动了物联网领域的兴起。然而，这一新兴领域也正面临着前所未有的信息安全挑战：个人隐私、物品信息等随时都可能被泄露，远程控制他人物品，甚至操纵城市供电系统，夺取机场的管理权限都有可能发生。物联网的兴起可能引发很多新的信息安全问题，这些安全问题主要体现在以下几方面。

(1)感知节点的安全问题。由于感知节点数量庞大，往往分布在一个很大的区域内，所以当缺少有效监控时，攻击者可以轻易地接触到节点物理实体，并对它们进行破坏，甚至可通过本地操作轻易地替换节点的软硬件。

(2)感知网络的安全问题。通常情况下，感知节点所有的操作都依靠自身所携带的电池供电。它的计算能力、存储能力、通信能力受到节点自身所携带能源的限制，无法实现复杂的安全协议，因而也就无法拥有强大的安全保护能力。

(3)无线自组网的安全问题。自组网作为物联网的末梢网，由于其拓扑的动态变化会导致节点间信任关系的不断变化，所以给密钥管理造成了很大的困难。

(4)核心网络的信息安全问题。物联网的核心网络应当具有相对完整的安全保护能力，但是由于物联网中节点数量庞大，而且以集群方式存在，所以在数据传输时，会因大量节点发送数据而造成网络拥塞，从而影响网络的可用性。

(5)物联网业务的安全问题。由于物联网设备可能是先部署后连接网络，而物联网节点又无人看守，所以如何对物联网设备进行远程签约信息和业务信息配置就成了难题。

(6)射频识别(Radio Frequency Identification，RFID)系统安全问题。RFID系

统同传统的 Internet 一样，容易受到攻击，这主要是因为标签和读写器之间的通信是通过电磁波的形式实现的。此过程中没有任何物理或可视的接触，这种非接触和无线通信方式存在严重的安全隐患。因此，物联网在应用初期无疑会将更多的攻击目标直接或间接地暴露给黑客，并为黑客提供更多的攻击途径。

随着云计算和大数据时代的到来，互联网将释放出海量数据，因此产生、存储、分析的数据量越来越大。海量数据背后隐藏着大量的经济与政治利益，而通过数据挖掘，人类所表现出的数据整合与控制力量远超以往。图 1-1 所示为大数据时代的数据金字塔，数据经过整合、分析与挖掘之后逐步转化为信息、知识乃至情报，数据的价值和其指导意义也随之显著提高。大数据如同一把双刃剑，社会因大数据使用而获益匪浅，但个人隐私也无处遁形。近年来，侵犯个人隐私的案件频频发生，例如，2010 年谷歌泄露 Wi-Fi 网络用户信息达 6 亿多字节，2010 年美国电信运营商 AT&T 泄露 11.4 万用户姓名和邮箱信息，2011 年韩国门户网站泄露 3500 万用户信息，2012 年盛大发生云数据丢失事件等。2013 年 6 月，美国国家安全局前雇员爱德华·斯诺登曝光了包括“棱镜”在内的美国政府多个秘密监视项目。尽管美国及其盟友铺设的全球监控网一直是个公开的秘密，但此次曝光揭露的监视范围之广、程度之深和数据量之大，仍引起全世界震惊。这些事件严重侵犯了用户的合法权益。专家指出，“网络安全是当今人类遭遇的最大安全问题”。

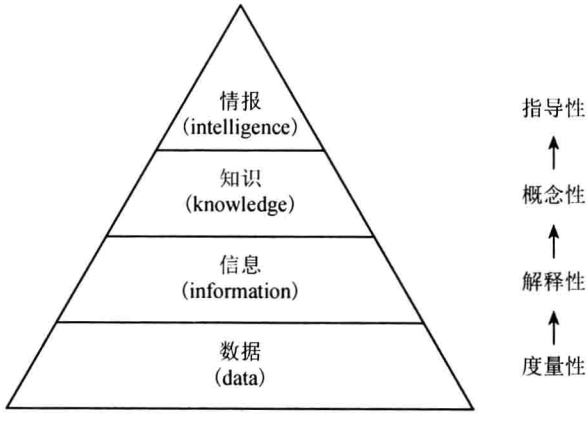

图 1-1 大数据时代的数据金字塔

云计算和大数据时代侵犯个人隐私有以下表现。

(1)在数据存储的过程中对个人隐私权造成的侵犯。云服务中用户无法知道数据确切的存放位置，用户对其个人数据的采集、存储、使用、共享无法有效控制。这可能会因不同国家的法律规定而造成法律冲突问题，也可能产生数据混同和数据丢失。

(2)在数据传输的过程中对个人隐私权造成的侵犯。云环境下数据传输将更为开放和多元化，传统物理区域隔离的方法无法有效保证远距离传输的安全性，电磁泄漏和窃听将成为更为突出的安全威胁。

(3)在数据处理过程中对个人隐私权造成的侵犯。云服务商可能部署大量的虚拟技术，基础设施的脆弱性和加密措施的失效可能产生新的安全风险。大规模的数据处理需要完备的访问控制和身份认证管理，以避免未经授权的数据访问，但云服务资源动态共享模式无疑增加了这种管理的难度，如账户劫持、攻击、身份伪装、认证失效、密钥丢失等都可能威胁用户数据安全。

(4)在数据销毁过程中对个人隐私权造成的侵犯。单纯的删除操作不能彻底销毁数据，云服务商可能对数据进行备份，同样可能导致销毁不彻底，而且公权力也会对个人隐私和个人信息进行侵犯。为满足协助执法的要求，各国法律通常会规定服务商的数据存留期限，并强制要求服务商提供明文的可用数据，但在实际应用中，很少受到收集限制原则的约束，公权力与隐私保护的冲突也是用户选择云服务需要考虑的风险点。因此，在云计算和大数据时代，要切实加强个人隐私保护，防止敏感信息泄露。

1.1.3　信息安全问题的发展方向

1)云计算和大数据安全

云计算和大数据应用的兴起，为企业发展开拓了新的方向，但大量数据的集中管理，也成了黑客攻击的明显标靶。2013 年 6 月“棱镜门”事件的爆发，使得大数据安全防护问题成为了社会热议话题，越来越多的人认识到大数据安全的重要性。时至今日，已有的信息安全防护技术和产品尚不能为大数据应用提供完备的安全防护，现有的信息安全保护技术在为大数据的机密性、完整性、可用性提供安全有效的保障上已经出现了缺漏。作为未来发展的主流应用，云计算和大数据是信息技术领域的最新热点之一。云计算和大数据安全已成为当前热议的话题，也必将成为未来信息安全领域的主要发展和研究方向之一。

2)物联网安全

与传统网络相比，物联网的感知节点大都部署在无人监控的环境下，具有能力脆弱、资源受限等缺点，并且由于物联网是在现有的网络基础上扩展了感知网络和应用平台，传统网络安全措施不足以提供可靠的安全保障，从而使得物联网的安全问题具有特殊性。物联网领域的兴起必将直接或间接地将更多的攻击目标直接暴露在黑客面前，为黑客攻击系统提供更多的突破口和途径。如何提高节点自身的安全性和抗攻击能力，构建安全的网络管理和通信协议，对于物联网安全的广泛应用具有重要意义，这将成为信息安全领域的一个重要研究方向。

3)硬件体系架构安全

硬件作为软件执行的支撑平台,其安全性是上层软件安全的重要前提和基础。然而传统的硬件体系架构在设计时并未考虑系统的安全需求。缓存、分支预测器、多核等高性能结构的引入,使得硬件架构中隐含越来越多的隐通道,并增加了软件通过共享资源发生相互干扰的可能,为黑客攻击系统提供了新的突破口。此外,随着集成电路生产和销售链的全球化,硬件在设计和生产的过程中可能嵌入恶意代码,成为黑客攻击系统的后门。McAfee 实验室在其发布的《2012 年威胁预测报告》中指出:“嵌入式硬件将成为黑客新的攻击方向……。”[3]从硬件底层为系统构建可信、可靠和可验证的安全基础,并为上层软件提供安全属性的度量、控制与验证能力,也将成为未来信息安全领域的重要发展方向之一。

4)工业和基础设施安全

随着信息技术的迅猛发展,信息化在生产和服务企业中的应用取得了飞速发展,互联网技术的出现,使得工业控制网络和基础设施中大量采用通用 TCP/IP 技术,工业控制系统(Industrial Control System,ICS)网络和企业管理网的联系越来越紧密。随着信息化和工业化深度融合的推进,网络化管理操作成为重要的发展趋势,同时也使得针对工业控制系统与关键基础设施的病毒和木马攻击呈现出攻击来源复杂化、攻击目的多样化,以及攻击过程持续化的特征。2010 年,伊朗核电站的震网病毒攻击事件即是一个典型的例子[4]。此外,传统工业控制系统和基础设施采用专用的硬件、软件与通信协议,设计上基本没有考虑互联互通所必须考虑的通信安全问题。企业管理网与工业控制网的防护功能都很弱,甚至几乎没有隔离功能,因此在工业控制系统和基础设施开放的同时,也减弱了系统与外界的隔离,工业和基础设施的安全隐患日益突出。

5)安全关键系统

近年来,随着汽车电子、生物医疗设备等安全关键系统(safety-critical system)智能化程度的不断提高,这些系统往往都具备与外界进行通信的能力,而这些安全关键系统在设计时并没有考虑信息安全问题。相关文献报道:黑客可通过无线信道对汽车内部网络[5]、心脏起搏器[6]、胰岛素泵[7]等安全关键设备实施攻击,并能够远程控制这些设备的运行状态。如何提高这些安全关键系统的抗干扰和抗攻击能力是信息安全领域的一个新的研究方向。

物联网、云计算、大数据等领域的兴起给信息系统带来了前所未有的安全挑战,大数据、传感器网络、工业和基础设施、安全关键系统正面临着严重的网络安全威胁。本书以硬件安全为侧重点,对普遍应用于工业和基础设施的高可靠系统信息安全问题进行探讨,并给出一种对高可靠系统软硬件关键安全属性进行测试与验证的方法。