中国科学: 信息科学 2016 年 第 46 卷 第 2 期: 125–164
SCIENTIA SINICA Informationis
《中国科学》杂志社
SCIENCE CHINA PRESS

评 述

网络空间安全综述

张焕国[①*], 韩文报[②], 来学嘉[③], 林东岱[④], 马建峰[⑤], 李建华[⑥]

① 武汉大学计算机学院, 武汉 430072
② 数学工程与先进计算国家重点实验室, 无锡 214122
③ 上海交通大学计算机系, 上海 200240
④ 信息工程研究所, 北京 100093
⑤ 西安电子科技大学网络与信息安全学院, 西安 710071
⑥ 上海交通大学信息安全工程学院, 上海 200240
* 通信作者. E-mail: liss@whu.edu.cn

收稿日期: 2015–08–06; 接受日期: 2015–09–29; 网络出版日期: 2016–01–22
国家自然科学基金 (批准号: 2014CB340601, 61332019, 61379139, U1135002, U1405255, 61431008, 2013CB329603) 资助项目

摘要 随着信息技术的发展与广泛应用, 人类社会进入信息化时代. 在信息时代, 人们生活和工作在网络空间中. 网络空间是所有信息系统的集合, 是人类生存的信息环境. 因此, 必须确保网络空间的安全. 本文综合介绍网络空间的概念、网络空间安全学科、密码学、网络安全、信息系统安全和信息内容安全领域的研究发展、存在的问题和一些研究热点.

关键词 网络空间安全 信息安全 密码学 网络安全 信息系统安全 信息内容安全

1 概念

1.1 网络空间的概念

人类社会在经历了机械化、电气化之后, 进入了一个崭新的信息化时代. 在信息时代, 信息产业成为第一大产业. 信息就像水、电、石油一样, 与所有行业和所有人都相关, 成为一种基础资源. 信息和信息技术改变着人们的生活和工作方式. 离开计算机、网络、电视和手机等电子信息设备, 人们将无法正常生活和工作. 因此可以说, 在信息时代人们生存在物理世界、人类社会和信息空间组成的三维世界中 [1~4].

为了刻画人类生存的信息环境或信息空间, 人们创造了 Cyberspace 一词. 然而 Cyberspace 一词在我国的译名尚不统一. 如有信息空间、网络空间、网电空间、数字世界等, 甚至还有译音: 赛博空间.

早在 1982 年, 加拿大作家 William Gibson 在其短篇科幻小说《燃烧的铬》中创造了 Cyberspace 一词, 意指由计算机创建的虚拟信息空间, Cyber 在这里强调电脑爱好者在游戏机前体验到交感幻觉, 体现了 Cyberspace 不仅是信息的聚合体, 也包含了信息对人类思想认知的影响. 此后, 随着信息技术的快速发展和互联网的广泛应用, Cyberspace 的概念不断丰富和演化.

引用格式: 张焕国, 韩文报, 来学嘉, 等. 网络空间安全综述. 中国科学: 信息科学, 2016, 46: 125–164, doi: 10.1360/N112015-00176

2008 年, 美国第 54 号总统令对 Cyberspace 进行了定义: Cyberspace 是信息环境中的一个整体域, 它由独立且互相依存的信息基础设施和网络组成. 包括互联网、电信网、计算机系统、嵌入式处理器和控制器系统.

目前, 国内外对 Cyberspace 还没有统一的定义. 我们认为它是信息时代人们赖以生存的信息环境, 是所有信息系统的集合. 因此把 Cyberspace 翻译成信息空间或网络空间是比较好的. 其中信息空间突出了信息这一核心内涵, 网络空间突出了网络互联这一重要特征. 本文主要采用网络空间这一名称.

1.2 网络空间安全的概念

信息安全是信息的影子, 哪里有信息哪里就存在信息安全问题.

从信息论角度来看, 系统是载体, 信息是内涵. 网络空间是所有信息系统的集合, 是人类生存的信息环境, 人在其中与信息相互作用相互影响. 因此, 网络空间存在更加突出的信息安全问题. 其核心内涵仍是信息安全.

当前, 一方面是信息技术与产业的空前繁荣, 另一方面是危害信息安全的事件不断发生. 敌对势力的破坏、黑客攻击、恶意软件侵扰、利用计算机犯罪、隐私泄露等, 对信息安全构成了极大威胁. 除此之外, 科学技术的进步也对信息安全提出新的挑战. 由于量子和 DNA 计算机具有并行性, 从而使得许多现有公钥密码 (RSA、ELGamal、ECC 等) 在量子和 DNA 计算机环境下将不再安全. 因此, 网络空间安全的形势是严峻的 [5,6].

对于我国来说, 网络空间安全形势的严峻性, 不仅在于上面这些威胁, 更在于我国在 CPU 芯片和操作系统等核心芯片和基础软件方面主要依赖国外产品. 这就使我国的网络空间安全失去了自主可控的基础.

习近平主席指出: “没有网络安全, 就没有国家安全. 没有信息化, 就没有现代化”. 我们必须确保我国的网络空间安全.

2 网络空间安全学科

2.1 网络空间安全学科的内涵

传统的信息安全强调信息 (数据) 本身的安全属性, 认为信息安全主要包含:

- 信息的秘密性. 数据不被未授权者知晓的属性.
- 信息的完整性. 数据是正确的、真实的、未被篡改的、完整无缺的属性.
- 信息的可用性. 数据是随时可以使用的属性.

信息论的基本知识告诉我们, 信息不能脱离它的载体而孤立存在, 因此我们不能脱离信息系统而孤立地谈论信息安全. 这也就是说, 我们应当从信息系统的角度来全面考虑信息安全. 据此, 我们把信息系统安全划分为 4 个层次: 设备安全、数据安全、内容安全、行为安全. 其中数据安全即是传统的信息安全 [1~4].

1. 设备安全. 信息系统设备的安全是信息系统安全的首要问题.

- 设备的稳定性. 设备在一定时间内不出故障的概率.
- 设备的可靠性. 设备能在一定时间内正常执行任务的概率.
- 设备的可用性. 设备随时可以正常使用的概率.

信息系统的设备安全是信息系统安全的物质基础, 如果失去了这个物质基础, 信息系统安全就变成空中楼阁. 对信息设备的任何损坏都将危害信息系统的安全.

2. 数据安全. 采取措施确保数据免受未授权的泄露、篡改和毁坏.

- 数据的秘密性. 数据不被未授权者知晓的属性.
- 数据的完整性. 数据是正确的、真实的、未被篡改的、完整无缺的属性.
- 数据的可用性. 数据是随时可以使用的属性.

信息系统的设备安全是信息系统安全的物质基础, 但是仅仅有信息系统的设备安全是远远不够的. 必须在设备安全的基础之上, 进一步确保数据安全.

3. 内容安全. 内容安全是信息安全在政治、法律、道德层次上的要求.

- 信息内容在政治上是健康的;
- 信息内容符合国家法律法规;
- 信息内容符合中华民族优良的道德规范.

除此之外, 广义的内容安全还包括信息内容保密、知识产权保护、信息隐藏和隐私保护等诸多方面.

4. 行为安全. 数据安全是一种静态安全, 行为安全是一种动态安全.

- 行为的秘密性. 行为的过程和结果不能危害数据的秘密性. 必要时, 行为的过程和结果也应是秘密的.
- 行为的完整性. 行为的过程和结果不能危害数据的完整性, 行为的过程和结果是预期的.
- 行为的可控性. 当行为的过程出现偏离预期时, 能够发现、控制或纠正.

行为安全的思想符合哲学上实践是检验真理唯一标准的基本原理, 同时也符合我国政府的 “安全、可控” 的信息安全策略.

确保信息安全是一个系统工程, 必须综合采取各种措施才能奏效. 特别应当强调的是, 绝不能忽视法律、教育、管理措施, 在许多情况下它们的作用大于技术措施.

信息系统的硬件系统安全和操作系统安全是信息系统安全的基础, 密码和网络安全等技术是关键技术. 而且, 只有从信息系统的硬件和软件的底层做起, 从整体上综合采取措施, 才能比较有效地确保信息系统的安全 [1~4,7~9].

综上, 我们给出网络空间安全学科的定义: 网络空间安全学科是研究信息获取、信息存储、信息传输和信息处理领域中信息安全保障问题的一门新兴学科 [7~9].

网络空间安全学科是计算机、电子、通信、数学、物理、生物、管理、法律和教育等学科交叉融合而形成的一门交叉学科. 它与这些学科既有紧密的联系, 又有本质的不同. 信息安全学科已经形成了自己的内涵、理论、技术和应用, 并服务于信息社会, 从而构成一个独立的一级学科. 2015 年 6 月国务院学位委员会和教育部批准增设网络空间安全一级学科.

2.2 网络空间安全学科的主要研究方向和研究内容

当前, 网络空间安全学科的主要研究方向有: 密码学、网络安全、信息系统安全、信息内容安全和信息对抗 [7~9].

(1) 密码学. 密码学由密码编码学和密码分析学组成, 其中密码编码学主要研究对信息进行编码以实现信息隐蔽, 而密码分析学主要研究通过密文获取对应的明文信息. 密码学的主要研究内容有

(a) 对称密码;

(b) 公钥密码;

(c) Hash 函数;

(d) 密码协议;

(e) 新型密码 —— 生物密码、量子密码等;

(f) 密钥管理;

(g) 密码应用.

(2) 网络安全. 网络安全的基本思想是在网络的各个层次和范围内采取防护措施, 以便能对各种网络安全威胁进行检测和发现, 并采取相应的响应措施, 确保网络环境的信息安全. 其中, 防护、检测和响应都需要基于一定的安全策略和安全机制. 网络安全的主要研究内容有

(a) 网络安全威胁;

(b) 通信安全;

(c) 协议安全;

(d) 网络防护;

(e) 入侵检测;

(f) 入侵响应;

(g) 可信网络.

(3) 信息系统安全. 信息系统是信息的载体, 是直接面对用户的服务系统. 用户通过信息系统得到信息的服务. 信息系统安全的特点是从系统级的整体上考虑信息安全的威胁与防护. 信息系统安全的主要研究内容有

(a) 信息系统的安全威胁;

(b) 信息系统的硬件系统安全;

(c) 信息系统的软件系统安全;

(d) 访问控制;

(e) 可信计算;

(f) 信息系统安全等级保护;

(g) 信息系统安全测评认证;

(h) 应用信息系统安全.

(4) 信息内容安全. 信息内容安全是信息安全在政治、法律、道德层次上的要求. 我们要求信息内容是安全的, 就是要求信息内容在政治上是健康的, 在法律上是符合国家法律法规的, 在道德上是符合中华民族优良的道德规范的. 信息内容安全的主要研究内容有

(a) 信息内容的获取;

(b) 信息内容的分析与识别;

(c) 信息内容的管理和控制;

(d) 信息内容安全的法律保障.

目前学术界对信息内容安全的认识尚不一致. 广义的信息内容安全还包括信息内容的保密、知识产权保护、信息隐藏、隐私保护等.

(5) 信息对抗. 信息对抗是, 为消弱、破坏对方电子信息设备和信息的使用效能, 保障己方电子信息设备和信息正常发挥效能而采取的综合技术措施, 其实质是斗争双方利用电磁波和信息的作用来争夺电磁频谱和信息的有效使用和控制权. 信息对抗的主要研究内容有

(a) 通信对抗;

(b) 雷达对抗;

(c) 光电对抗;
(d) 计算机网络对抗.

2.3 网络空间安全学科的理论基础

网络空间安全学科在其形成和发展过程中形成了自己特有的学科理论基础和方法论 [7~9].

(1) 数学是一切自然科学的理论基础, 当然也是信息安全学科的理论基础.

现代密码可以分为两类: 基于数学的密码和基于非数学的密码. 但是, 基于非数学的密码 (如量子密码和 DNA 密码等) 正处在发展的初期, 尚没有广泛的实际应用. 目前广泛应用的密码仍然是基于数学的密码. 对于基于数学的密码, 密码学界普遍认为设计一个密码就是设计一个数学函数, 而破译一个密码就是求解一个数学难题. 这就从本质上清晰地阐明了数学是密码学的理论基础. 作为密码学理论基础之一的数学分支主要有代数、数论、概率统计、组合数学等.

协议是网络的核心, 因此协议安全是网络安全的核心. 作为协议安全理论基础之一的数学主要有逻辑学等.

博弈论是现代数学的一个分支, 是研究具有对抗或竞争性质的行为的理论与方法. 一般, 称具有对抗或竞争性质的行为为博弈行为. 在博弈行为中, 参加对抗或竞争的各方各自具有不同的目标或利益, 并力图选取对自己最有利的或最合理的方案. 博弈论研究的就是博弈行为中对抗各方是否存在最合理的行为方案, 以及如何找到这个合理方案. 博弈论考虑对抗双方的预期行为和实际行为, 并研究其优化策略. 博弈论的思想古已有之, 我国古代的《孙子兵法》不仅是一部军事著作, 而且是最早的一部博弈论专著. 博弈论已经在经济、军事、体育和商业等领域得到广泛应用. 信息安全领域的斗争无一不具有这种对抗性或竞争性. 如, 网络的攻与防、密码的加密与破译、病毒的制毒与杀毒、信息隐藏与分析、信息对抗, 等等. 因为信息安全领域的斗争, 本质上都是人与人之间的攻防斗争, 因此博弈论便成为网络空间安全学科的基础理论.

(2) 信息论、控制论和系统论是现代科学的基础, 因此也是网络空间安全学科的基础理论.

信息论是商农为解决现代通信问题而创立的; 控制论是维纳在解决自动控制技术问题中建立的; 系统论是为了解决现代化大科学工程项目的组织管理问题而诞生的. 它们本来都是独立形成的科学理论, 但它们相互之间紧密联系、互相渗透, 在发展中趋向综合、统一, 有形成统一学科的趋势. 这些理论是信息安全学科的基础理论.

信息论奠定了密码学和信息隐藏的基础. 信息论对信息源、密钥、加密和密码分析进行了数学分析, 用不确定性和唯一解距离来度量密码体制的安全性, 阐明了密码体制、完善保密、纯密码、理论保密和实际保密等重要概念, 把密码置于坚实的数学基础之上, 标志着密码学作为一门独立的学科的形成. 因此, 信息论成为密码学的重要的理论基础之一.

从信息论角度看, 信息隐藏 (嵌入) 可以理解为在一个宽带信道 (原始宿主信号) 上用扩频通信技术传输一个窄带信号 (隐藏信息). 尽管隐藏信号具有一定的能量, 但分布到信道中任意特征上的能量是难以检测的. 隐藏信息的检测是一个有噪信道中弱信号的检测问题. 因此, 信息论构成了信息隐藏的理论基础.

系统论是研究系统的一般模式、结构和规律的科学. 系统论的核心思想是整体观念. 任何一个系统都是一个有机的整体, 不是各个部件的机械组合和简单相加. 系统的功能是各部件在孤立状态下所不具有的.

控制论是研究机器、生命社会中控制和通信的一般规律的科学. 它研究动态系统在变化的环境条件下如何保持平衡状态或稳定状态. 控制论中把 “控制” 定义为, 为了改善受控对象的功能或状态, 获

得并使用一些信息, 以这种信息为基础施加到该对象上的作用. 由此可见, 控制的基础是信息, 信息的传递是为了控制, 任何控制又都依赖于信息反馈.

信息安全遵从 “木桶原理”. 这 “木桶原理” 正是系统论的思想在信息安全领域的体现.

保护、检测、响应 (PDR) 策略是确保信息系统和网络系统安全的基本策略. 在信息系统和网络系统中, 系统的安全状态是系统的平衡状态或稳定状态. 恶意软件的入侵打破了这种平衡和稳定. 检测到这种入侵, 便获得了控制的信息, 进而杀灭这些恶意软件, 使系统恢复安全状态.

确保信息系统安全是一个系统工程, 只有从信息系统的硬件和软件的底层做起, 从整体上综合采取措施, 才能比较有效地确保信息系统的安全.

以上观点已经经过信息安全的实践检验, 证明是正确的, 是行之有效的. 它们符合系统论和控制论的基本原理. 这表明, 系统论和控制论是信息系统和网络系统安全的基础理论.

(3) 网络空间安全学科的许多问题是计算安全问题, 因此计算理论也是网络空间安全学科的理论基础, 其中包括可计算性理论和计算复杂性理论等.

可计算性理论是研究计算的一般性质的数学理论. 它通过建立计算的数学模型, 精确区分哪些是可计算的, 哪些是不可计算的. 对于判定问题, 可计算性理论研究哪些问题是可判定问题, 哪些问题是不可判定问题.

计算复杂性理论使用数学方法对计算中所需的各种资源的耗费作定量的分析, 并研究各类问题之间在计算复杂程度上的相互关系和基本性质. 可计算理论研究区分哪些是可计算的, 哪些是不可计算的, 但是这里的可计算是理论上的可计算, 或原则上的可计算. 而计算复杂性理论则进一步研究现实的可计算性, 如研究计算一个问题类需要多少时间, 多少存储空间. 研究哪些问题是现实可计算的, 哪些问题虽然是理论可计算的, 但因计算复杂性太大而实际上是无法计算的.

众所周知, 授权是信息系统访问控制的核心, 信息系统是安全的, 其授权系统必须是安全性的. 可计算性的理论告诉我们: 一般意义上, 对于给定的授权系统是否安全这一问题是不可判定问题, 但是一些 “受限” 的授权系统的安全问题又是可判定问题. 由此可知, 一般操作系统的安全问题是一个不可判定问题, 而具体的操作系统的安全问题却是可判定问题. 又例如, 著名的 “停机问题” 是不可判定问题, 而具体程序的停机问题却是可判定的. 由此可知, 一般计算机病毒的检测是不可判定问题, 而具体软件的计算机病毒检测又是可判定问题. 这就说明了可计算理论是信息系统安全的理论基础之一.

本质上, 密码破译就是求解一个数学难题, 如果这个难题是理论不可计算的, 则这个密码就是理论上安全的. 如果这个难题虽然是理论可计算的, 但是由于计算复杂性太大而实际上不可计算, 则这个密码就是实际安全的, 或计算上安全的. “一次一密” 密码是理论上安全的密码, 其余的密码都只能是计算上安全的密码. 根据计算复杂性理论的研究, NPC 类问题是 NP 问题中最难计算的一类问题. 公钥密码的构造往往基于一个 NPC 问题, 期望密码是计算上安全的. 如 McEliece 密码基于纠错码的一般译码是 NPC 问题. 背包密码基于求解一般背包问题是 NPC 问题. MQ 密码基于多变量二次非线性方程组的求解问题是 NPC 问题, 等等. 这说明计算复杂性理论是密码学的理论基础.

(4) 访问控制理论是网络空间安全学科的理论基础.

访问控制是信息系统安全的核心问题. 访问控制的本质是, 允许授权者执行某种操作获得某种资源, 不允许非授权者执行某种操作获得某种资源. 许多信息安全技术都可看成是访问控制. 例如, 网络等信息系统中的身份认证是最基本的访问控制. 密码技术也可以看成是访问控制. 这是因为, 在密码技术中密钥就是权限, 拥有密钥就可以执行相应密码操作获得信息. 没有密钥, 就不能执行相应密码操作不能获得信息. 同样, 信息隐藏技术也可以看成是访问控制. 这是因为, 在信息隐藏中隐藏的技术与方法就是权限, 知道了隐藏的技术与方法, 就能获得隐藏的信息. 不知道隐藏的技术与方法, 就不能获得

隐藏的信息.

访问控制理论包括各种访问控制模型与授权理论. 例如, 矩阵模型、BLP 模型、BIBA 模型、中国墙模型、基于角色的模型 (RBAC)、属性加密等等. 其中属性加密是密码技术与访问控制结合的新型访问控制.

访问控制是信息安全领域的一种共性关键技术, 许多信息安全领域都要应用访问控制技术. 因此, 访问控制理论是网络空间安全学科的理论基础, 而且是网络空间安全学科所特有的理论基础.

(5) 密码学理论是网络空间安全学科的理论基础.

虽然信息论奠定了密码学的基础. 但是, 密码学在其发展过程中已经超越了传统信息论, 形成了自己的一些新理论. 如单向陷门函数理论、公钥密码理论、零知识证明理论、多方安全计算理论、以及部分密码设计与分析理论. 从应用角度看, 密码技术是信息安全的一种共性技术, 许多信息安全领域都要应用密码技术. 因此, 密码学理论是网络空间安全学科的理论基础, 而且是网络空间安全学科特有的理论基础.

综上可知, 数学 (代数、数论、博弈论等)、信息理论 (信息论、系统论、控制论)、计算理论 (可计算性理论、计算复杂性理论) 是网络空间安全学科的理论基础, 而博弈论、访问控制理论和密码学理论是网络空间安全学科所特有的理论基础.

2.4 网络空间安全学科的方法论基础

Decare 在 1637 年出版了著作《方法论》, 研究论述了解决问题的方法, 对西方人的思维方式和科学研究方法产生了极大的影响. Decare 把研究的方法划分为 4 步:

(a) 永不接受任何我自己不清楚的真理. 对自己不清楚的东西, 不管是什么权威的结论, 都可以怀疑.

(b) 将要研究的复杂问题, 尽量分解为多个比较简单的小问题, 一个一个地解决.

(c) 将这些小问题从简单到复杂排序, 先从容易解决的问题入手.

(d) 将所有问题解决后, 再综合起来检验, 看是否完全, 是否将问题彻底解决了.

Decare 的方法论强调了把复杂问题分解成一些细小的问题分别解决, 是一种分而治之的思想. 但是它忽视了各个部分的关联和彼此影响. 近代科学特别是系统论的发展使我们发现, 许多复杂问题无法分解, 分解之后的局部并不具有原来整体的性质, 因此必须用整体的思想和方法来处理, 由此导致系统工程的出现. 方法论由传统的方法论发展到系统性的方法论.

网络空间安全学科的方法论既包含分而治之的传统方法论, 又包含综合治理的系统工程方法论, 而且将这两者有机地融合为一体. 具体概括为, 理论分析、逆向分析、实验验证、技术实现 4 个核心内容 [7~9], 这四者既可以独立运用, 也可以相互结合, 指导解决信息安全问题, 推动网络空间安全学科发展. 在运用这些方法论分析和解决信息安全问题时, 特别强调底层性和系统性. 即, 根据信息安全学科方法论的指导, 从信息系统的软硬件底层和系统结构层来分析和解决信息安全问题.

逆向分析是网络空间安全学科所特有的方法论. 这是因为信息安全领域的斗争, 本质上是攻防双方之间的斗争. 《孙子兵法》指出: “知己知彼, 百战不殆”. 知彼就是要逆向分析. 信息安全学科的每一分支都具有攻和防两个方面. 如密码学由密码编码学和密码分析学组成, 网络安全由网络安全防护和网络攻击组成等等. 因此必须从攻和防两个方面进行研究. 例如, 在密码学的研究中, 既要研究密码设计又要研究密码分析. 在网络安全的研究中, 既要研究网络安全防护又要研究网络攻击. 而且在进行网络安全防护设计时, 首先要进行安全威胁分析和风险评估. 这些都是逆向分析方法论的具体应用, 并且已被实践证明是正确的和有效的.

在设计和分析信息系统安全时, 不仅涉及到技术, 还涉及到系统的组织管理和法律保障等诸多方面. 除此之外, 因为人是系统的管理者和使用者, 因此人是影响信息系统安全的重要因素. 又因为信息安全领域对抗的本质是人与人之间的对抗, 而人是最智能的. 不考虑人的因素, 是不可能有效解决信息安全问题的.

因此, 我们应当, 以人为核心, 运用定性分析与定量分析相结合、注意量变会引发质变、综合处理、追求整体效能, 解决信息安全中的理论、技术和应用问题.

3 密码学

密码学是研究如何在敌手存在的环境中保护通信及信息安全的科学. 密码学的公开研究时间较短, 标志性事件是 1949 年 Shannon《保密系统的通信理论》的发表以及 20 世纪 70 年代美国 DES 算法的公布和公钥密码思想的提出. 之后公开密码研究发展迅速, AES、NESSIE 计划、eSTREAM 计划、SHA3 计划以及 CAESAR 计划极大地推动了密码学新思想、新方法的发展. 此外, 云计算、大数据等新的应用环境, 侧信道攻击等新的攻击手段带来了新的安全需求. 于是, 涌现出了全同态密码、属性及函数密码、程序混淆密码、抗泄露密码等新的研究方向. 下面我们从密码算法、密码协议、密码实现、密钥安全 4 个方面介绍密码学研究现状及进展情况, 并介绍值得关注的研究热点.

3.1 密码算法

密码算法主要包括分组密码、流密码、Hash 函数及 MAC、公钥密码以及新兴的认证加密算法等. 20 世纪 70 年代, 美国国家标准局 NBS 发布数据加密标准 DES. 但随着网络的发展和计算能力的提高, DES 密钥长度过短的劣势逐渐暴露出来. 在 1999 年的 RSA 竞赛中, Distributed. net 组织利用 10 万台普通计算机协同工作在 1 天之内通过穷举搜索获得了 DES 密钥. 为了取代 DES, 美国标准技术研究所 NIST 发起了征集高级加密标准 AES 的竞赛, 经过三轮筛选从初始 15 个候选算法中确定 Rijndael 算法作为 AES. AES 可以抵抗包括差分攻击、线性攻击等已知的各种攻击手段, 且在软硬件实现速度、内存要求方面都具有很好的性质. AES 发布后, 理论研究的重点转为对现有密码结构安全性分析, 并取得了一系列重要的成果 [10~12]. 分组密码研究中一个值得注意的新方向是在现实应用中有广泛需求的轻量级密码得到了快速发展. 比如 PRESENT [13], LBlock [14], PRINCE [15], PRIDE [16], Simplified AES [17] 等及针对这些新轻量级算法的一系列分析工作.

20 世纪初, 代数攻击的出现给基于 LFSR 设计的流密码算法带来巨大威胁, 2003 年结束的 NESSIE 计划竟然没有一个流密码通过安全性评估被选为标准. 由于流密码可通过分组密码工作模式的调整得到, 以 Shamir 为代表的很多学者提出应该全面检讨是否还有必要再单独设计流密码. 但流密码领域的学者普遍认为在软件上可以快速实现的流密码或在硬件实现上只需要很少资源的流密码依然具有实用价值. 于是, 欧盟 ECRYPT 项目在 2004 年发起了称为 eSTREAM 的流密码设计竞赛, 最终选出了 4 个软件可快速实现的流密码: HC-128, Rabbit, Salsa20, SOSEMANUK, 以及 3 个对硬件资源要求低的流密码算法: Grain v1, MICKEY v2, Trivium. eSTREAM, 计划大大促进了流密码设计分析思想的发展. 在设计方面, 新的研究动向有二: 一是开始出现非线性乱源设计; 二是分组密码的设计思想逐步融入流密码设计. 在分析方面也取得了一些新进展 [18,19], 出现了针对 LFSR 的快速相关攻击 [20]、区分攻击 [21]、高阶差分攻击 [22] 以及立方攻击 [23] 等. 我国学者在流密码理论研究 [24,25] 及设计方面成果颇丰, 特别需要指出的是由我国学者设计的祖冲之密码 [26] 在 2011 年入选为 LTE 国际标准, 大

大提升了我国在新一代无线通信领域的话语权.

Hash 函数是一个将任意长度的消息映射成固定长度消息的函数, 带密钥的 Hash 函数也称为 MAC. Hash 函数和 MAC 可用于认证和数字签名, 具有非常重要的实际应用, 如 2012 年的火焰病毒就是因为攻击者获得了 Windows 系统升级程序使用的 Hash 算法的碰撞, 从而可以对自身代码进行数字签名, 使杀毒软件认为病毒拥有合法数字证书, 从而绕过杀病毒软件的查杀. 由于我国学者王小云在 MD5, SHA-1 等 Hash 函数攻击方面取得突破性进展 [27~30], 2007 年 NIST 启动了 SHA-3 计划, 在全球范围内征集新的 Hash 标准, 最终 Keccak 算法被选为 SHA-3 算法. SHA-3 计划促进了 Hash 函数和 MAC 的快速发展, 涌现了 HAIFA、SPONG、宽管道、双管道等多种新的结构和设计方法, 同时其分析方法也出现了新的进展 [31~34]. 近年来, 在 Hash 函数和 MAC 设计方面, 实用同态 MAC [35] 是一个值得注意的新方向.

认证加密是近年新兴的研究领域, 目标是利用单一密码同时提供机密性、完整性与认证功能. 认证加密方案可通过分组密码的 OCB、CCM 模式来构造, 但其存在一定的效率瓶颈. 2013 年, NIST 启动了 CAESAR 竞赛 [36], 掀起了直接构造完整的认证加密方案的热潮. 已经提出了诸多认证加密方案, 如 ALE、FIDES、AEZ 等 [37~43], 但密码学界对这个新兴领域的安全问题认识尚不完全透彻, 以致出现了不少安全问题 [44~47]. 可以预见, 认证加密方案的研究将成为未来几年里最受关注的研究方向之一.

自 1976 年 Diffie 与 Hellman 提出公钥密码概念以来, 提出了许多公钥密码体制, 目前应用最为广泛的包括 RSA 密码、ElGamal 密码和椭圆曲线密码. 但公钥密码的密钥证书管理比较复杂, 为了简化密钥管理, Shamir 提出了基于身份的公钥密码 [48], Boneh 和 Franklin 基于双线性配对技术构造了实用的方案 [49]. 随后, 很多优秀的基于身份方案 [50~53] 陆续提出. 出现了新型的公钥密码体制, 如无证书加密 [54]、广播加密 [55,56]、属性加密 [57~60]、谓词加密 [61,62], 及函数加密 [63,64] 等. 其中属性加密、谓词加密、函数加密等已成为解决云计算环境下数据安全及隐私保护问题的重要技术手段.

由于 shor 量子算法的提出, 传统的基于大整数分解和离散对数问题的公钥密码的安全受到了巨大的威胁, 研究能够抵抗量子计算攻击的公钥密码成为急需. 称能够抵抗量子计算机攻击的密码为抗量子计算密码. 目前认为抗量子计算密码主要有 3 类: 基于物理学的量子密码、基于生物学的 DNA 密码和基于数学的抗量子计算密码. 其中基于数学的抗量子计算密码目前主要有: 多变量密码体制、纠错码密码体制、格公钥密码体制和基于 Hash 函数的签名体制 [5].

3.2 密码协议

密码协议是指两方或者更多方, 为完成某种信息系统安全功能而执行的一系列规定步骤. 由于面向应用, 密码协议的涵盖非常广泛, 既包括身份认证、密钥交换、秘密共享、数字签名、零知识证明、多方安全计算等基本工具, 也包括电子选举、电子投票等复杂功能.

秘密共享的概念最早由 Shamir 和 Blakley 分别提出, 目的是希望将一个秘密分解后交给多人掌管, 只有在秘密持有人达到设定人数时, 秘密才能被恢复. Shamir 使用了 Lagrange 插值法来实现秘密共享, Blakley 使用多维空间中的点来进行构造. 秘密共享协议一直在不断发展 [65], 又出现了线性秘密共享及近来的函数秘密共享 [66]. 目前, 秘密共享已经成为构造更复杂密码协议 [67,68] 的基本工具.

零知识证明是指证明者向验证者证明他知道某个秘密而同时又不泄露秘密的任何信息的一种方法. 这一概念最早由 Goldwasser 等 [69] 于 1985 年提出, 通过证明者和验证者之间的一系列交互来实现. 随后, Santis 等解决了不需要交互的零知识证明问题 [70,71]. Deng 等解决了零知识证明中的双重可重置猜想问题 [72,73]. Zhao 等实现了公钥环境下的并发零知识协议 [74]. 零知识证明是各类安全

协议的基础, 已经被广泛用于身份认证、电子投票等协议的设计中. 近年来, 又有一些新的模型和方法 [75,76] 用在特定应用领域 [77] 的零知识证明中.

安全多方计算是一个由多方参与的分布式计算协议, 每个参与方分别提供输入信息参与计算, 并获得计算结果, 但在计算结束后, 却无法获得其他参与方的输入信息. 安全多方计算最初由姚氏百万富翁问题 [78] 引出, 有两方参与计算, 后推广成为多方计算 [79]. 安全多方计算使用秘密共享、零知识、比特承诺 [80]、不经意传输 [81] 等作为其基础工具, 以构造电子选举协议、电子拍卖协议等应用协议, 并且在门限签名、数据库查询与数据挖掘、隐私保护中有很重要的应用. 早在 1997 年, Goldwasser 就对安全多方计算进行了比较全面的总结 [82], 近年来, 安全多方计算理论依然在缓步发展. 如新出现的黑盒安全多方计算 [83]、计算过程可中止的安全多方计算 [84], 及非交互式安全多方计算 [85] 等新的方法值得研究者关注.

随着各种新型网络及应用的出现, 出现了如外包计算 [86,87]、可验证存储 [88,89] 等新的应用协议. 随着云计算、物联网、车载网、互联网 +、智慧城市等更广泛的应用, 密码协议设计及分析方法的研究也必将获得新的发展.

3.3 密码实现安全

密码算法分数学形态、软件形态和硬件形态, 通常说密码算法是安全的是指密码算法在数学上是安全的, 但密码算法的应用必须以软件或硬件的形态实现, 而数学上的安全并不能保证算法的软硬件实现安全.

侧信道攻击是一种利用与密码实现有关的物理特性来获取运算中暴露的秘密参数, 以减少理论分析所需计算工作的密码分析方法. 1996 年, Kocher 首次提出了侧信道攻击方法, 利用测量密码算法执行时间的方法成功分析了 RSA 和 DES 算法 [90~92]. 随后, 差错 [93,94]、能量 [95]、辐射 [96,97]、噪声、电压等更多物理特性 [98,99] 被用于侧信道分析技术中. 特别值得指出的是, 我国的谷大武、周永彬、唐明等在侧信道攻击研究方面也取得了优异的成果. 为抵抗侧信道攻击, 研究人员提出了指令顺序随机化、加入噪声、掩码、随机延迟等方法, 但都无法完全抵抗越来越复杂的各种侧信道攻击.

2008 年, Petite 等 [100] 提出在设计算法时就需要考虑信道泄露信息情况下算法的安全性, 并设计了一个简洁的流密码算法, Dziembowski 与 Pietrzak 进一步提出了抗泄露密码 [101] 这一概念, 将可能泄露的信道信息抽象为数学上的泄露函数. 这就把物理实现上存在的问题重新归纳为数学问题. 在这种模型下设计出的算法自然可以避免实现时可能遇到的安全问题. 在这种思路下, 近年来出现很多在不同应用目标下的抗泄露密码算法 [102~105], 成为密码学领域的一项新的重要研究方向. Yu 等在该方面作出了很好的工作 [106,107].

另一方面, 在很多应用中攻击者可以侵入系统获取密码系统的密钥, 称这种攻击为白盒攻击. 一种抵抗白盒攻击的方法称为白盒实现, 它是将密钥做成查询表分发到整个网络结构中, 使得每个块看起来独立于密钥, 攻击者无法从中直接获得密钥数据. 已经提出了一些白盒实现 [108,109], 但同时也出现了若干攻击 [110], 可以说目前还未有公认的安全高效的白盒密码实现. 2013 年密码混淆技术 [111] 取得重大进展以来, 提出了基于密码混淆技术的白盒密码, 但其效率成为瓶颈. 混淆技术将可能成为保证密钥和密码算法代码安全的一种方法.

3.4 密钥管理

密钥为密码系统中最重要的资源, 对密码系统最有效的攻击为直接获取密钥. 密钥管理的目标是

保证密钥的全生命周期的安全, 包括密钥的产生、分配、存储、使用、备份/恢复、更新、撤销和销毁等环节的安全.

密钥一般需要随机生成, 弱的随机数发生器将直接导致密码系统安全性降低. 2013 年 Snowdon 曝出, NSA 设计了带陷门的伪随机数生成算法 Dual_EC_DRBG 并通过 NIST 确立为标准, 之后买通 RSA 公司, 将该算法作为 Bsafe 安全软件中的默认随机数生成算法, 从而对世界进行信息控制. 此外, 通过对网络上大量使用的 RSA 密码算法的模数进行大量扫描再两两求取公因子, 研究人员得到了诸多 RSA 密码系统的私钥从而进行破解, 这主要也是因为使用随机数发生器生成 RSA 私钥时, 不同系统 RSA 私钥之间发生了碰撞.

如前所述, 密钥通常由随机数产生器生成, 包括真随机数发生器 (TRNG) 和伪随机数发生器 (PRNG) 两类. TRNG 通过物理环境的随机因素来产生随机性, 近年来研究热点集中在高速 TRNG 的设计 [112]、安全分析及熵估计理论 [113,114] 方面. PRNG 是由随机种子通过确定性算法扩展得到随机性. 无论是 TRNG 还是 PRNG, 使用之前都必须进行安全性分析和检测.

随着目前嵌入式设备、可穿戴设备的广泛应用, 如何保护这些设备中的私钥成为关键问题. 物理不可克隆 (PUF) [115] 技术提供了密钥生成及存储保护的一体化解决方案. 该技术利用物理芯片本身的结构指纹, 在每次需要密钥运算时, 结合一个密钥生成算法临时提取私钥, 保证断电后无法通过物理入侵的手段直接读取密钥. 目前出现了诸多低成本高可靠的 PUF 设计, 但其安全性分析和安全应用 [116] 还需进一步研究.

目前通信网络模型下的密钥管理技术已较为成熟, 包括层次化的密钥结构、标准化的密钥协商协议、采用硬件或加密方式存储密钥、采用秘密共享或密钥托管方式存储或恢复密钥. 公钥密码的密钥管理技术 PKI 也已经成熟. 但是, 密钥管理技术与具体应用紧密相关, 必须针对具体应用才能设计出合理的密钥算理方案. 云计算、物联网、大数据等新的应用环境给密钥管理提出更多新需求和新挑战, 研究这些新兴应用下的密钥管理技术成为重要的研究方向.

3.5 研究热点

本节介绍密码学领域的几个研究热点, 它们或者有望发展为重大新研究方向, 或者有望解决重大密码学问题, 包括抗量子计算密码、格密码、全同态密码、程序混淆密码、属性及函数密码、密码设计与分析自动化等.

目前认为抗量子计算密码主要有 3 类: 基于物理学的量子密码、基于生物学的 DNA 密码和基于数学的抗量子计算密码. 在量子密码中最成熟的是量子密钥分配, 其安全性基于量子力学基本原理, 可提供无条件安全的密钥分配. 我国在这一领域的研究和应用处于国际前列. 应当指出, 量子密码不是只有量子密钥分配, 还有量子分组密码和量子公钥密码. 但是后者受量子计算复杂性理论的限制, 尚不成熟, 需要投入更多的研究. 由于 DNA 密码不是基于计算的, 所以它具有抵抗量子计算机攻击的能力. 我国学者提出了 DNA 对称和公钥密码方案 [117,118]. 但是目前的 DNA 密码主要基于实验技术, 缺少理论基础, 设计和应用都不够方便. 这些都需要进一步深入研究. 基于数学的抗量子计算密码目前主要有: 多变量密码体制、纠错码密码体制、格公钥密码体制和基于 Hash 函数的签名体制. 其中格密码和多变量密码的研究比较多. 研究表明, 目前许多多变量密码方案是不安全的, 设计出安全高效的多变量密码是困难的. 而格密码兼具安全性和效率优势, 被认为是目前最有前途的抗量子计算密码体制.

量子密码中目前最成熟的是量子密钥分配 (QKD) 协议. 迄今人们已经提出了基于不同物理原理、传输介质和编码方式的多种 QKD 协议, 包括 BB84 协议 [119]、B92 协议 [120]、EPR 协议 [121]、差分相

位协议 (DPS) [122]、相干单向协议 (COW) [123]、连续变量协议 [124]、反直觉协议 [125] 等. 其中 BB84 协议的安全性得到公认. 尽管 QKD 协议具有理论上的绝对安全, 但由于现实中器件是非理想的, 目前 QKD 协议的热点逐步转向与实际系统结合的安全性研究, 包括测量设备无关 QKD 协议 [126]、半设备无关 QKD 协议 [127]、完全设备无关 QKD 协议 [128] 等. 必须指出, 量子密码绝非只有量子密钥分配, 还有量子加密、签名、认证等其他密码, 但这些密码尚不成熟, 亟待进一步深入研究.

格中困难问题具有最坏情形与平均情形困难性相等和被普遍认为抗量子计算攻击两大优势, 此外在全同态加密设计中也发挥重要作用 [129,130]. 目前, 格中困难问题已被用来构造标准 CPA, CCA- 安全公钥加密体制 [131,132]、基于身份的加密体制 [133~135]、数字签名体制 [136~139]、密钥协商协议 [140]、盲传输协议 [141]、Hash 函数 [142] 等. 此外理想格 [143] 的引入使得基于格的密码体制开始日趋实用. 尽管如此, 由于格中问题的具体困难性并不完全明晰, 相较 RSA, ECC 等公钥密码体制, 对格公钥密码进行安全性评估以及较精确的参数选择更为困难, 这些方面还需要进一步研究.

全同态加密允许在未知密钥情况下, 对密文进行任意操作, 其所得的值解密后等于对相应明文进行相同操作后所得的值, 由于其特殊的 “同态” 性质, 因此在云计算等环境中具有非常重要的应用. 全同态加密思想早在 1978 年就由 Rivest 等提出, 但直到 2009 年才由 Gentry 提出第一个全同态加密方案 [144]. 之后涌现出了大量全同态加密的设计, 目前效率最高的全同态加密方案的构造都主要基于理想格上的 LWE 问题 [145,130]. 在美国 DARPA 实施的 “密文可编程” 项目支持下, 全同态加密在快速实现上出现重大突破 [146~149], 计算效率相对原有 Gentry 方案提升了 5∼6 个数量级, 密钥量也从 GB 降低到 MB 量级, 尽管如此, 其效率离大规模实际应用仍有一定的距离. 另外, 提高同态密码的安全性, 也是一个值得研究的方面.

程序混淆密码在保留程序功能性的同时使得程序是 “不可识别” 的, 其最初主要通过一些启发式方法实现. 2001 年 Barak 等 [121] 首次对程序混淆给出了严格的密码学定义并进行系统研究. 2013 年 Grag 等 [111] 在通用不可区分混淆的构造上取得重大突破以来, 研究人员以程序混淆为工具成功构造了可否认加密 [150]、标准模型下可证安全的全域 Hash 方案 [151] 等, 解决了诸多密码学困难难题, 同时也出现了新的通用混淆设计方法 [152,153], 但其构造与安全性归约都十分复杂, 效率较低. 最近, 由于构造程序混淆的基本工具 —— 多线性映射相继被攻击 [154,155], 研究人员可能需要对程序混淆密码进行重新审视.

属性加密的密文和密钥都与一组属性相关, 加密者可以指定接收者的属性, 使得产生的密文只能由满足加密策略的属性用户解密, 具有一对多的加解密模式. 函数加密为属性加密的推广, 加密者不但能够决定用户能否解密数据, 还能够决定用户能够解密什么形式 (函数) 的数据. 由于可实现灵活的细粒度访问控制, 属性和函数加密成为当前大数据、云存储环境中加密数据访问控制的重要工具, 并成为密码学领域的研究热点.

众所周知, 安全强度高是对密码的基本要求. 然而高安全强度密码的设计却是十分复杂困难的. 如何设计出高安全强度的密码和使密码设计自动化是人们长期追求的目标. 文献 [156,157] 最先研究利用智能计算设计密码函数, 为密码函数的设计自动化走出了重要的一步. 文献 [158,159] 将密码学与智能计算结合起来, 借鉴生物进化的思想, 提出了演化密码的概念和利用演化密码实现密码设计和密码分析自动化的方法. 文献 [3] 总结了这方面的研究成果. 近年来已经出现了量子智能算法. 我国学者利用量子智能算法设计密码函数, 在多指标优化方面取得好成绩. 应当指出, 密码是一个复杂系统, 密码设计和分析自动化决非易事. 但是, 在社会信息化的今天, 应当让计算机在密码设计与分析中发挥越来越大的作用.

4 网络安全

4.1 网络安全需求

近年来, 随着无线网络、智能终端、云计算等新兴技术的快速发展, 以物联网、5G 网络、CPS 等为代表的下一代网络 [160] 正处于逐步部署和实现过程中, 网络形态逐步呈现出了层次化、虚拟化、服务化的特点. 在下一代网络中, 网络安全是保障整个系统正常工作, 提供多样化应用服务的基础, 其面临着来自不同层次的各种威胁和挑战. 针对不同层次的安全需求, 国内外学者通过设计安全协议、构建攻击防护、访问控制和隐私保护等安全机制来实现网络环境下信息的安全采集、传输、存储和服务.

4.2 网络安全机制

4.2.1 安全协议

网络依托协议构建起来, 因此, 安全协议贯穿于网络的各层, 是网络安全的基础. 根据不同网络层次安全需求, 国内外学者在形式化方法的支撑下设计了多种类型的安全协议.

在感知层中, 密钥分发协议的设计是实现节点认证、加密通信的基础协议, 目前是感知层安全协议研究的热点. 针对传感网节点数量大、能量受限等特点, 预分发密钥是当前无线传感网中采用的主流方案, 比较典型的协议有 BROSK 协议 [161]、ZigBee 协议 [162] 以及 LKMS [163] 协议等, 易于部署但安全性较差. 对此, 有学者提出了任意两个传感器节点共享不同密钥的方案 [164], 安全性较高, 但存储代价较高. 综合安全和效率, 采用密钥链的方式可以让每个节点储存多个密钥, 从而减小密钥规模. 基于密钥链的典型协议包括 Gupta 等 [165] 的随机分发密钥链的方案, Huang 等 [166] 的基于簇首的密钥分发方案, 此外, 还有基于哈希链的改进方案 [167]、多路径的改进方案 [168] 以及密钥重分发的方案 [169] 等多个方案. 在传感网安全路由协议设计方面, 主要采用针对特定的攻击对标准路由协议进行扩展, 从而保证数据路由过程中的安全性.

在传输层中, 结合 TCP/IP 传输协议簇模型, 安全协议的设计由下至上主要包括接入认证、安全路由、端到端安全传输、异构网络安全切换及漫游等协议. 在接入认证方面, 由于无线网络的开放性, 使其更易遭受攻击, 因此, 现有研究主要集中在无线网络环境下. 目前 WLAN 的认证协议通常基于 802. 1x 访问控制架构 [170] 和 EAP 协议规范 [171] 来进行设计和分析的, 在 IETF 标准中, 典型协议包括 EAP-MD5, EAP-LEAP, EAP-TLS, EAP-PEAP, EAP-AKA 等 [172]. MD5 方法最简单, 但安全性较低; EAP-TLS 使用 PKI 来保护认证过程, 被认为是最安全的认证方法, 但由于交互过程复杂而导致验证开销较大, 对此, Li 等 [173] 设计了两轮交互消息完成 4 步握手协议, 在保证安全性的同时大大提高了效率. 此外, 随着用户对隐私保护需求的提升, 匿名认证协议的设计和实现也成为安全领域的研究热点 [174,175]. 在安全路由、端到端安全传输协议设计方面, 以 IPSec, SSL/TLS 安全协议为代表. IPSec 定义了数据在路由过程中使用的安全功能, 引入密钥管理协议 IKE 来实现实体间动态认证, 并生成后续通信过程中的会话密钥 [176]. SSL/TLS 采用 X.509 认证, 并使用认证过程中产生的会话密钥保证两个应用间端到端通信的机密性和可靠性 [177]. 根据不同的应用场景, 研究者在这两种典型协议的基础上又作了许多扩展和改进. 在异构网络安全切换及漫游方面, 许多学者以 LTE-WLAN 互联体系作为典型场景进行了研究, 包括 3GPP 组织提出的 TS 33.234 [178], 基于椭圆曲线密码的快速认证协议 [179]. 基于 WAPI 的匿名网络接入协议等 [180]. Zhao 等设计了一种 OAKE 协议, 在安全性、效率等方面优于美国的 MQV/HMQV 协议 [181].

在汇聚层和应用层中, 网络攻击主要针对数据和应用软件, 系统通过攻击防护、访问控制和隐私保护等机制来保证信息的安全性, 协议则作为载体用来部署和实施所提出的安全机制.

4.2.2 网络攻击防护

网络的开放性和共享性以及协议和软件的安全漏洞决定了网络中面临着多层次、多种类的安全攻击. 根据攻击对象的不同, 可以分为针对网络协议和针对服务应用的攻击两种.

针对网络协议的攻击主要集中在感知层和传输层. 在感知层中, 针对传感节点能量受限、安全机制弱等缺陷, 攻击者可以实施射频干扰、节点俘获、碰撞和耗尽攻击、虚假路由信息攻击、选择性转发攻击、黑洞攻击、女巫攻击和虫洞攻击等 [182~184]. 通过使用认证、加密、监听、探索、发送冗余数据包以及采用多径路由可以抵御上述的攻击 [185]. 在传输层, 存在的典型网络攻击包括 SYN 洪泛和 TCP 会话劫持等. 使用防火墙技术来检测和过滤数据, 可以有效地抵御 SYN 洪泛攻击 [186]. 使用 SSL 等安全通信协议, 可以有效抵御 TCP 会话劫持.

针对服务应用的攻击主要集中在汇聚层和应用层, 主要包含针对应用服务器的网络攻击和恶意软件入侵. 针对应用服务器的攻击包括 DoS 攻击, 以及针对特定协议的攻击, 如 DNS 缓存投毒 [187]. 通过部署防火墙, 配置安全策略, 即可保护应用服务器抵御网络攻击. 恶意软件包括病毒、蠕虫、木马、rootkits 和僵尸网络 [188]. 恶意软件检测技术用来保护系统免受恶意软件的危害. 恶意软件的检测技术分为基于异常的检测技术、基于规则的检测技术和基于特征的检测技术 [189]. 根据检测方法, 每种检测技术又可以分为动态检测、静态检测和混合检测.

4.2.3 访问控制

访问控制在众多领域中有着重要的应用. 网络系统是一种复杂分布式系统, 用户及资源种类众多, 不同的用户对不同的资源 (网络、数据和服务) 有不同的操作权限, 因此需要根据安全需求制定相应的安全策略来保证信息安全和业务的正常运转.

在感知层和传输层中, 访问控制通常与安全认证协议及用户身份管理相结合, 主要应用在用户接入认证方面, 如 802.1x 访问控制框架. 在该框架下, 只有通过验证的用户和节点才能够正常使用相应的网络资源.

在汇聚层和应用层中, 访问控制根据相应安全策略对用户访问数据和服务资源的权限进行验证. 在访问控制机制研究中, 核心是安全策略的设计, 根据策略种类的不同, 常见的访问控制模型包括基于角色的访问控制模型 RBAC [190], 基于任务和行为的访问控制模型 TBAC [191]. 在 RBAC 模型中, 权限根据用户身份进行分配. TBAC 采用动态授权的主动安全模型, 根据用户/程序的行为实时进行权限管理. 但 RBAC 和 TBAC 可扩展性不高, 属于粗粒度的访问控制. 为此, Goyal 等 [192] 提出了基于属性的访问控制模型 (ABAC), 控制策略是基于请求者和资源所固有的一些属性, 并将网络环境等因素考虑进去, 使得 ABAC 具有足够的灵活性和可扩展性, 同时使得安全的匿名访问成为可能. 此外, 随着大数据时代的到来, 多数据源信息服务下细粒度的访问控制成为未来研究的热点 [193].

4.2.4 隐私保护

近年来, 随着城市信息化建设的加快, 隐私问题越来越受到人们的关注. 目前, 在网络环境下, 根据不同的隐私保护需求分为两类: 一类是针对网络链路信息的保护, 如发送/接收者信息、路由信息等; 另一类针对网络中的敏感数据保护.

针对网络链路信息的保护主要针对感知层和传输层 [194]. 信息传输过程中, 攻击者会跟踪数据传输路径从而获得用户的一些隐私信息, 因此, 通常通过设计安全路由协议来保护用户的隐私信息. 路由协议隐私保护方法一般基于随机路由策略, 即数据包的每一次传输并不都是从源节点向汇聚节点方向传输, 而是转发节点以一定的概率将数据包向远离汇聚节点的方向传输. 同时传输路径不是固定不变的, 每一个数据包的传输路径都随机产生. 所以, 这样的随机路由策略使得攻击者很难获取数据传输的真实路径, 从而无法获取用户的隐私信息.

针对敏感数据信息的保护贯穿于网络中的每个层次, 目前保护敏感数据的方法主要包括以下两类: 一种通过修改或隐藏原始信息的局部或全局敏感数据来保护隐私, 主要的方法有 k- 匿名 [195]、l- 多样性 [196]、差分隐私 [197] 等; 另一种是通过加密技术对信息进行保护, 主要的方法有同态加密技术、安全多方计算等. 在感知层, 隐私保护主要包括节点内部的隐私保护和整个传感器网络的隐私保护 [198]. 在传输层, 结合传输层安全协议采用加密技术实现数据隐私保护. 在汇聚层, 主要采用 k- 匿名、l- 多样性、差分隐私等方法实现用户敏感信息的隐藏. 在应用层, 主要针对服务过程中的信息隐私保护, 如位置隐私等; 近年来, 随着服务组合技术的发展, 信息流控制技术被用于信息在不同服务间交互时的隐私保护 [199].

4.3 未来网络安全研究方向

随着互联网技术的广泛应用, 网络正向泛在互联、移动化、智能化、可定制、更高速化的方向发展, 其中存在的安全隐患则不同于传统网络安全问题, 需要结合新的技术和背景进行研究. 本节针对目前具有代表性的 5 个网络安全发展方向进行讨论, 为未来网络安全的发展提供参考.

4.3.1 移动终端安全

随着硬件和软件技术的不断更新, 移动终端已经能够提供与个人 PC 相似或相同的功能, 逐渐成为具有强大便携和计算能力的个人智能系统. 通过多种网络接入技术, 例如 IEEE 802. 11、蓝牙、GSM、GPRS、UMTS 等, 移动终端能够实现不同环境下与不同设备的互联, 并随时共享信息. 然而, 丰富的网络接入方式导致了移动设备容易成为恶意软件和用户的攻击目标. 目前针对移动终端主流的攻击方式包括: 无线攻击 (wireless attacks) [200,201]、入侵攻击 (break-in attacks) [202,203]、面向基础设施的攻击 (infrastructure-based attacks) [204,205]、蠕虫攻击 (worm-based attacks)、僵尸网络 (Botnet) 和基于用户的攻击 (user-based attacks) [206,207].

4.3.2 网络设备安全

随着网络设备逐渐向智能化方向发展, 原有计算系统中的安全问题也存在于网络设备当中. 例如, 智能路由设备, 其操作系统可能受到恶意用户的攻击而使路由错误转发或失效, 导致网络不可用. 以路由器为例, 其面临的主要安全威胁包括: DDOS 攻击 (distributed denial of service attack)、中间人攻击 (man in the middle attack) [208,209]、TCP 重置攻击 (TCP reset attack) [210] 以及针对 OSPF 的攻击 (attack on OSPF) [211~213].

4.3.3 SDN 安全

由于传统因特网把控制逻辑和数据转发紧耦合在网络设备上, 导致网络控制平面管理的复杂化, 也使网络控制层面的新技术很难直接部署在现有网络上, 灵活性和扩展性较差. 而 SDN (software

defined networking) 将逻辑控制和数据转发进行分离, 减少了网络设备承载的诸多复杂功能, 提高了网络新技术和新协议实现和部署的灵活性和可操作性. 因此, SDN 能够提供灵活可定制的网络拓扑结构以及虚拟网络设备, 能够有效监控网络数据的传输, 并支持不同协议的安装和卸载等.

然而灵活性也为 SDN 带来了安全方面的威胁. 文献 [214] 认为 SDN 的安全需求主要发生在应用层和控制层之间, 包括: (1) 应用的授权、认证、隔离; (2) 策略冲突的消解. 针对应用的授权、认证、隔离问题, 文献 [214,215] 给出了相应的分析和解决方案. 文献 [216] 提出了一种安全加固的控制平面操作系统, 用以解决策略冲突消解的问题. 文献 [217] 提出了一个在 SDN 架构上开发网络安全应用的开发环境 FRESCO, 保证了基于 SDN 应用开发的安全.

4.3.4 CPS 安全

信息物理融合系统 (CPS) 是通过计算 (computation)、通信 (communication) 与控制 (control) 技术的有机与深度融合, 实现计算资源与物理资源的紧密结合与协调的下一代智能系统. CPS 是由运行在不同时间和空间范围的分布式的、异步的异构系统组成的动态混合系统. 由于 CPS 具有跨层、异构、高度互联等特点, 因此其面临的安全问题和挑战也呈现较为复杂的特性. 文献 [218] 提出了 CPS 面临的主要 6 个安全挑战, 包括: 机密性、上下文模糊、安全聚合、拓扑模糊、可扩展信任管理与隐私聚合. 文献 [219] 从 CPS 安全目标和威胁、安全需求、主要攻击手段、安全关注点、安全问题解决方案 5 个方面阐述了 CPS 安全研究领域的主要内容. 文献 [220~222] 分别从安全策略、安全平台、安全协议等方面论述了 CPS 系统设计和运行中的安全问题, 并给出了相应的解决方法.

4.3.5 5G 网络安全

5G 并不是单一的无线接入技术, 也不是几个全新的无线接入技术, 而是多种新型无线接入技术和现有无线接入技术 (4G 后向演进技术) 集成后的解决方案总称. 从某种程度上讲, 5G 是一个真正意义上的融合网络. 5G 终端设备拥有软件定义的无线收发与调制方式以及新的错误控制模式. 终端设备能够同时接入和访问多种不同的无线网络, 并能够根据服务访问的需求自动进行网络的切换. 文献 [223] 提出 5G 安全挑战主要包含可重构、自适应并且轻量级保护机制的设计以及预防来自应用层的攻击行为. 由于 5G 技术是当前新兴通信和网络技术的融合, 文献 [224] 提出 5G 的安全挑战实质上来自其组成部分, 例如 SDCN 安全、无线网络融合安全、D2D、M2M 安全等.

5 信息系统安全

5.1 可信计算的新发展

5.1.1 中国可信计算的新发展

中国的可信计算, 起步不晚, 水平不低, 成果可喜, 处于国际可信计算领域的前列 [1,2,4,225~228].

1. 中国的可信计算标准

2013 年中国公布了以下 3 个可信计算技术标准. 这些标准反映了中国可信计算技术的新进展.

(1) 可信平台主板功能接口 (GB/T 29827-2013)

可信平台主板功能接口标准的核心创新是, 改进 TCG 的 TPM, 设计了我国的可信平台控制模块 TPCM [4]. TPCM 的主要技术创新点是:

• 将可信度量根 RTM、可信存储根 RTS 和可信报告根 RTR 都集中到 TPCM 中, 以 TPCM 作为平台的信任根.

TCG 的 RTM 是 BIOS 开始部分的软件代码, 由于 RTM 置于 TPM 之外, 容易受到恶意攻击. 将它放到 TPCM 中, 提高了安全性.

• 具备主动的度量功能. 平台启动时 TPCM 首先掌握对平台的控制权, 并对平台关键部件进行完整性度量.

TCG 的可信计算平台在启动时首先执行 RTM. 因此, RTM 的执行是由平台的 CPU 执行的, 而这时尚未对平台进行可信度量, 因此 RTM 的执行有可能是不可信的. 采用主动度量机制后, 系统启动时 TPCM 首先掌握系统的控制权, RTM 的执行和信任度量都由信任根 TPCM 进行, 确保平台可信度量的安全.

• 配置中国商用密码算法的硬件引擎.

TPCM 在密码算法方面遵从中国《可信计算平台密码技术方案 (TCM)》, 并且配置中国商用密码算法 (SM2, SM3, SM4) 的硬件引擎, 提高了密码的处理速度.

• 为了提高 TPCM 对操作系统和应用程序的支持, 采用了高速的 PCI 或 PCI-E 总线作为 TPCM 与系统之间的连接.

TCG 的可信 PC 规范采用 LPC 总线实现 TPM 与平台的南桥芯片相连. 我们认为这是 TCG 为了与现有计算机兼容而采取的技术方案. 由于 LPC 总线的速率低, 不能支持高速的应用. TPCM 采用了高速的 PCI 或 PCI-E 总线, 能够对操作系统和应用程序提供更有力的支持.

• 增强身份认证功能. 通过 7816 总线实现口令与智能卡相结合的身份认证, 还可以扩展指纹等方式的身份认证.

可信平台模块有了 7816 总线后, 就可以方便地支持智能卡, 因此就能够实现口令与智能卡相结合的双因素身份认证. 这对提高平台的安全性是有利的.

• 通过 I2C 或 GPIO 等总线实现 TPCM 对计算机资源 (如 I/O 接和网络设备等) 的控制.

我国的信息安全政策是 “安全、可控”. 因此, 可信平台模块应当能够控制平台的资源, 这是设计 TPCM 的主要动机.

TPCM 的这些创新点是有充分的实践基础的. 早在 2003 年, 武汉大学与企业合作开发出的我国第一款可信计算机 (SQY14 嵌入密码型计算机) [229] 就已经实现了 TPCM 的主要创新点. SQY14 嵌入密码型计算机采用了一个嵌入式安全模块 (ESM) [230]. ESM 是由 J2810 芯片和中国商用密码芯片封装组成的模块, 因此 ESM 支持中国商用密码. ESM 通过 7816 总线控制智能卡子系统, 智能卡即是用户身份凭证又是用户密钥的载体. ESM 通过 I2C 总线控制计算机的重要资源 (如 BIOS) 和所有 I/O 端口, 实现了对计算机资源的主动管控. 在 ESM 内部开辟了日志, 与硬盘日志共同构成两级日志, 提高了日志的安全性. 实践已经证明, 这些安全措施对于提高 SQY14 嵌入密码型计算机的安全性是十分有效的 [229].

(2) 可信连接架构 (TCA) (GB/T 29828-2013)

可信网络连接 (TNC) 是 TCG 的一个重要规范. TNC 的目的是把平台的可信性向网络延伸, 确保网络的可信. 实践证明, TNC 具有开放性、安全性和系统性等优点. 但是, TNC 也有一些明显的不足:

• TNC 只有网络服务器对接入终端的验证, 缺少接入终端对网络服务器的验证. 显然, 网络服务器与接入终端是不对等的.

• TNC 中, 多个实体需要进行大量的信息交互, 却没有给出相应的安全协议, 只是简单的介绍了如何进行消息的传递.

• TNC 的架构比较复杂, 难于扩展, 实现成本高.

由于 TCA 的适用范围和场景与 TNC 相似, 因此在 TCA 规范的制定过程中, 参考了 TNC 规范和技术路线, 在发扬其优点的基础上, 同时注意克服其不足之处. TCA 具有以下几个创新点 [4]:

(a) TNC 本质上是一个二元架构, 网络服务器处于控制地位, 接入终端处于被动地位. 因此造成了只有网络服务器对接入终端的验证, 缺少接入终端对网络服务器的验证. TCA 采用了三元对等架构. 访问请求者和访问控制器作为对等实体, 策略管理器提供访问请求者与访问控制器之间双向的身份认证与平台可信性评估支持, 使得访问请求者与访问控制器一样具有控制连接的能力. 这种三元对等架构也使得 TCA 架构 3 个层次之间的协议与控制方式与 TNC 具有显著不同.

(b) 三元对等架构需要一个可信第三方为参与网络连接的两个对等实体进行身份认证与平台可信性评估. 在 TCA 中, 将策略管理器作为可信第三方, 实现对网络请求者与网络接入者之间的双向认证. 这种方式既简化了身份管理、策略管理和证书管理机制, 又保证了终端与网络的双向认证.

(c) TCA 架构基于我国自主知识产权的三元对等实体鉴别及访问控制方法, 在网络访问控制层采用三元鉴别可扩展协议 (TAEP) 实现 TCA 的实体鉴别, 支持序列 TAEP 鉴别和隧道 TAEP 鉴别两种实现方式. 采用三元对等鉴别的访问控制方法 (TePA-AC) 来实现端口访问控制, 支持全端口控制和部分端口控制两种实现方式.

(d) 为了降低系统实现难度, TCA 采用自底向上、支持完整实现的方式, 将 TCA 的协议进行统一定义, 在一个规范中包含了所有协议与接口功能的支持, 并通过自定义与保留字段的方式支持协议扩展. 从而使 TCA 产品设计人员容易理解所有的接口定义和协议流程.

(3) 可信计算密码支撑平台功能与接口规范 (GB/T 29829-2013)

TSS 软件栈是上层软件和 TPM 之间的软件中间件, 为上层软件使用 TPM 芯片提供了桥梁. 实践证明, TSS 具有安全性较好、效率高等优点, 总体上是成功的, 为可信计算发挥了重要作用. 但是, TSS 也存在一些不足之处:

(a) TCG 软件栈 TSS 规范在结构上采取了层次化和模块化的思想, 但是由于其在抽象层方面引入的对象实体较多, 导致关系复杂, 开发难度大. 另外, 这种结构对于嵌入式环境来说, 过于复杂, 因此不利于在嵌入式系统中应用.

(b) TSS 的主要目标是用于 TPM 的一般性管理与访问, 缺乏监控机制.

可信计算密码支撑平台功能与接口规范描述了可信计算密码支撑平台的功能原理与要求, 并定义了可信计算密码支撑平台为应用层提供服务的接口规范 [4]. 它与 TSS 规范的主要差异如下:

(a) 采用中国商用密码算法.

(b) 协议的精简及变化

• 使用自主设计的 AP 协议, 代替 TCG 的多个授权协议 (OIAP, OSAP 等);

• 协议中使用对称密码算法来保护请求和响应数据的秘密性;

• 由于存储保护使用对称密码算法, 存储主密钥为对称密钥, 因此密钥迁移协议也作了相应改动.

(c) 证书减少

TCG 的 TPM 1.2 使用 5 种证书, 而中国规范只使用两种证书: 密码模块证书和平台身份证书. 其中平台身份证书是双证书, 包括签名证书和加密证书.

(d) 密钥种类简少

TCG 的 TPM 1.2 使用 7 种密钥, 而中国规范只使用 4 种密钥: 密码模块密钥 EK、平台身份密钥 PIK、存储主密钥 SMK、用户密钥 UK.

2. 中国的 TCM/TPM 2.0 芯片

2012 年中国国民技术公司研制出世界上第一块 TCM/TPM 2.0 芯片, 支持中国商用密码算法, 通过国家密码管理局的认证, 并得到国内外的广泛应用.

3. 中国的麒麟操作系统

2013 年中国政府决定不采购 WIN-8 操作系统, 从而把用户对安全操作系统的紧迫需求和巨大市场提供给了中国企业.

我国中标软件公司开发出支持可信云计算的麒麟操作系统. 主要技术特征有支持可信启动 (TBOOT), 支持中国 TCM/TPM 2.0 芯片, 支持中国商用密码, 实现了从 TCM/TPM 到 VM 的完整信任链, 支持 Intel 的 TXT 技术和 OAT 技术, 实现了基于 OAT 的平台远程证明, 实现了可信云管理. 我们希望, 麒麟操作系统在进一步完善后走向实际应用.

5.1.2 TCG 可信计算的新发展

1. 从 TPM 1.2 到 TPM 2.0

随着可信计算技术的发展与应用, 特别是在了解到中国的 TCM 技术后, TCG 认识到在 TPM 设计方面存在的不足. TCG 从 2008 年开始考虑制定 TPM 的新规范, 经过几年的工作, 于 2012 年 10 月 23 日公开发布了 TPM 2.0 规范. TCG 在对 TPM 2.0 作了进一步的完善后, 于 2013 年向 ISO/IEC 提出 TPM 2.0 成为新标准的申请. 2015 年 6 月 ISO/IEC 接受 TPM 2.0 规范成为新的国际标准 [231]. 中国政府投了赞成票, 这说明 TPM 2.0 得到中国政府的认可.

TPM 2.0 与 TPM 1.2 相比, 作了许多改进, 其中最重要的是在密码配置与应用方面的改进.

(1) 密码配置更合理

• 支持多种密码算法. TPM 1.2 只配置了公钥密码, 没有明确配置对称密码. 公钥密码也只支持 RSA 密码. TPM 2.0 不仅支持公钥密码, 也支持对称密码. 对于公钥密码, 既支持 RSA, 也支持 ECC 和其他密码. 对于对称密码, 既支持 AES, 也支持其他密码. 对于 Hash 函数, 既支持 SHA-384 和 SHA-3, 也支持其他 Hash 函数.

• 支持密码算法更换. TPM 1.2 不支持密码算法更换. 在中国学者发现 SHA-1 的安全缺陷后 [27~30], 使得 TPM 1.2 的可用性下降. TPM 2.0 支持密码算法更换.

• 支持密码算法本地化. 由于 TPM 2.0 支持密码算法更换, 所以 TPM 2.0 支持各国使用自己的密码算法, 从而实现密码本地化. TCG 在 TPM 2.0 规范中, 特别强调了完全支持中国商用密码 SMx.

(2) 提高了密码性能

• TPM 1.2 只采用公钥密码 RSA, 没有采用对称密码, 因而加解密速度慢, 而且密钥证书种类多, 应用和管理不方便. 而 TPM 2.0 吸收了中国 TCM 的优点, 使用对称密码加密数据, 使用公钥密码进行签名和认证, 从而提高了密码处理速度, 而且减少了密钥证书的种类, 便于应用和管理.

• TPM 1.2 只支持 RSA 密码. 由于 RSA 密钥长, 软硬件实现规模大, 密码处理速度慢. TPM 2.0 既支持 RSA, 也支持 ECC 和其他密码. 由于 ECC 密钥短, 软硬件实现规模小, 密码处理速度快.

(3) 密钥管理更合理

• 密钥层次和类型. 从层次上划分, TPM 2.0 设置了 3 个密钥层次: 固件层、背书层和存储层. 其中固件层是 TPM 1.2 所没有的, 用以调用 BIOS 的密码资源, 从而增强了 TPM 2.0 的密码功能. 从功能上划分, TPM 2.0 有 3 种类型的密钥: 背书密钥 (EK)、存储密钥 (SK) 和认证密钥 (包含签名密钥和认证密钥).

• 减少了密钥和证书种类. TPM 1.2 定义了 7 种密钥和 5 种证书. 由于密钥和证书种类太多, 应用和管理都很复杂. 原因之一是, TPM 通过密钥类型定义密钥功能. 而 TPM 2.0 通过密钥功能定义密钥类型, 如定义一个签名密钥用于所有的签名, 从而减少了密钥的类型. 相应地, 证书的类型也就减少了.

• 密钥产生方案更合理. TPM 2.0 产生两种不同的密钥: 普通密钥和主密钥. 普通密钥用随机数产生器 (RNG) 产生. 主密钥的产生, 首先用 RNG 在 TPM 内部产生一个种子, 然后利用密钥派生函数 KDF 基于这个种子产生主密钥. TPM 2.0 采用了两种 KDF: 基于椭圆曲线的 ECDH SP800-56A 和基于 HMAC 的 KDF SP800-108.

(4) 支持虚拟化

• 云计算需要虚拟化, 而 TPM 1.2 不支持虚拟化. 为了使可信计算平台能够支持云计算, TPM 2.0 支持虚拟化.

(5) 提高了密钥使用的安全性

• 在 TPM 1.2 中, 如果密钥的授权数据是低熵的, 则易受到暴力攻击和中间人攻击. 又由于密钥的句柄是不被授权的, 攻击者可以盗用一个授权数据使用另外一个密钥, 从而危害密钥的安全性. 而 TPM 2.0 在授权数据中加入了秘密的辅助数据 (secret salt), 同时也改进了密钥句柄的授权, 增强了安全性.

• 在 TPM 2.0 中, 在 HMAC 中加入密钥的名称, 可以阻止密钥替换攻击, 从而提高了密钥的使用安全性.

(6) 统一授权框架

• TPM 1.2 中对应用、委托应用、迁移对象采用不同的授权方法, 管理复杂. TPM 1.2 中隐私保护模型也不一致, 有时使用 TPM 保护隐私, 有时又假定必须有操作系统的参与.

• TPM 2.0 采用了统一的授权框架, 而且扩展了授权方法, 允许利用签名和 HMAC 进行授权, 并允许进行组合.

虽然 TPM 2.0 与 TPM 1.2 相比, 作了许多改进, 安全性和可用性得到提高. 但是, TPM 2.0 仍然存在如下问题:

• TPM 2.0 的实际应用尚少, 它的安全性只有经过实践检验才能得到证实.

• TPM 2.0 支持密码算法更换, 支持密码本地化, 但是在这种多密码算法环境下的兼容性、安全性需要进行分析和验证.

• TPM 2.0 与 TPM 1.2 不兼容. 因此, 从 TPM 1.2 过渡到 TPM 2.0 需要一个较长的过渡时间.

由于 TPM 2.0 规范发布的时间不长, 而且 TCG 一直在对其进行修改. 所以, 学术界对它的研究还很少, 还需要进行深入的研究. 文献 [232] 对其密钥管理 API 进行了形式化分析, 文献 [233] 对其数字签名柔韧性和可升级性进行了研究. 文献 [232, 234] 发现 TPM 2.0 密钥复制机制的安全性问题, 并给出了安全增强方案. 文献 [235] 发现 TPM 2.0 策略授权机制的安全缺陷, 并给出了改进方案. 文献 [236] 发现在 TPM 2.0 中密钥数据块替换漏洞依然存在, 并指出结合应用程序的访问控制可在一定程度上规避该漏洞. 综上, TPM 2.0 规范是可信计算技术与产业发展的必然产物, 它的出现必将推动可信计算技术与产业的发展. 由此我们可以看到, 中国的可信计算对 TCG 的影响.

2. 从 VSTA 到 WIN-10

缺少操作系统对可信计算的支持, 是可信计算应用较少的主要原因之一 [1,2]. 微软公司长期致力于操作系统对可信计算的支持, 经历了从 VISTA 到 WIN-10 的发展历程. 由于 VISTA 过分强调了安全性, 忽视了易用性, 用户使用不方便, 结果用户不接受 VISTA. WIN-8 的开发吸取了 VISTA 的经验

和教训, 努力在提高安全性的基础上使用户使用方便. WIN-8 全面支持可信计算.

(1) 可信启动 (TBOOT). 基于 UEFI BIOS 和 TPM 2.0 芯片的支持, 实现了计算平台的可信启动. 而且, 可信启动中的可信度量, 由 TCG 规范中的简单 HASH 值度量, 增强为数字签名验证, 提高了安全性.

(2) 提前引入反病毒技术 (ELAM). 在可信启动过程中, 利用数字签名确保只有 Win-8 的 OS Laoder 被加载, 而且提前引入反病毒技术, 提高了安全性.

(3) 基于信誉的访问控制: 用户的信誉参与到访问控制中, 这有利于规范用户行为和营造和谐的应用环境.

(4) Bitlock 磁盘加密系统. WIN-8 保留了 WIN-7 的 Bitlock 磁盘加密系统, 而且利用 TPM 2.0 进行密钥管理, 提高了安全性.

由于操作系统是系统资源的管理者, 是信息系统安全的基础 [1,2,4,7], 出于确保我国信息安全的考虑, 中国政府决定不采购 WIN-8. 这一决定是十分正确的, 有利于国产操作系统技术与产业的发展.

尽管 WIN-8 全面支持可信计算, 增强了安全性, 但是用户对 WIN-8 仍不满意. 于是, 微软又开始研发 WIN-10, 并于 2015 年 7 月正式发布. WIN-10 在身份认证、数据保护、阻止威胁、设备安全等方面增强了安全性. 为了适应中国市场的应用, WIN-10 支持中国的 TCM/TPM 2.0 芯片. 用户是否喜欢 WIN-10, 只有通过应用才能知道.

5.2 云计算系统的安全

云计算是面向服务的计算, 通常划分为: 基础设施即服务 (IaaS)、平台即服务 (PaaS)、软件即服务 (SaaS). 云计算使计算象水、电、石油一样, 成为公共基础资源. 国际产业界普遍认为, 云计算是十大战略技术之首. 我国政府将云计算作为国家重点发展领域.

2012 年云成熟度调查结果表明, 41% 的用户拒绝采用云, 其主要原因是担心云的信息安全与隐私保护问题. 这说明, 信息安全与隐私保护问题已成为阻碍云计算发展的最大障碍!

由于云计算是面向服务的计算, 所以它必然采用资源共享的工作方式. 资源共享引出诸多的信息安全问题: 几乎无限的计算资源, 但用户不知道这些资源是否是可信的; 几乎无处不在的服务, 但用户不知道这些服务是否是可信的; 几乎无限的存储空间, 但用户不能感知自己数据的存在、更不能控制自己的数据. 于是, 用户对云计算不放心、担心自己的数据被损坏、被泄露、被篡改. 于是, 用户就不信任云计算.

可信计算是一种提高计算机系统可信性的信息安全技术. 而且可信计算特别适合用于提高信息系统的基础设施层和平台层的可信性. 因此, 采用可信计算来增强云计算的可信性, 是一种必然的选择.

5.2.1 IaaS 层的安全

基于可信计算增强云计算系统基础设施层的安全, 当前的研究主要集中在以下 4 个方面:

(a) 云计算系统的信任模型. 信任模型是可信计算技术的基础, 要基于可信计算增强云计算系统基础设施层的安全, 就必须首先建立云计算系统的信任模型. 为此, 应分析云计算系统的启动过程、软件加载和执行过程中的各部件的相互关系和相互作用, 特别是要分析虚拟机环境下的内部实体间的相互关系和相互作用. 进而研究其信任传递、度量与验证方法. 在此基础上, 建立云计算系统的信任模型.

(b) 云计算系统的可信计算基 (TCB). 分析云计算系统的安全威胁, 进而研究面对安全威胁的防护方法与防护体系. 其中的一个核心问题是作为云计算系统的安全基础的可信计算基 (TCB) 的构造. 有了可信计算基, 以此为信任基础, 逐级扩展信任关系, 最终可构建出可信云计算系统.

(c) 可信云计算系统的构建. 研究可信云计算系统的构建. 要特别考虑云计算的动态虚拟性给云计算系统构建带来的一些特殊安全问题.

(d) 云计算系统的安全监控. 研究云计算系统的安全监控. 特别是, 适应虚拟化和多租户任务执行环境下的安全监控机制与方法, 以确保云计算系统的运行安全.

文献 [237~239] 研究了 IaaS 层的动态完整性度量框架与协议, 并用实验证明了这些方法的可行性.

5.2.2 PaaS 层的安全

云操作系统和数据库等基础软件成为确保云计算安全的重要基础. 毫无疑问, 云操作系统和数据库等基础软件应当是支持可信计算的. 从微软公司 VISTA 到 WIN-10 走过的历程, 可知这是十分困难的. 尽管这件事是困难的, 但是人们仍然在坚定地前进. 这一点仍然可以从微软的 Windows 和我国中标麒麟操作系统的发展中看出, 参见 5.1.1 和 5.1.2 小节.

构造云可信执行环境, 为用户提供一个安全可靠的云平台是平台层的核心问题. 文献 [240] 研究了基于信任扩展的可信虚拟机执行环境构建方法. 文献 [241] 研究了基于 TPM 2.0 的虚拟可信平台及其安全性. 文献 [242] 研究了基于 vDRTM 支持多安全级别的可信执行环境 (TEE) 的构建. 文献 [243] 研究了对 TEE 中程序运行行为的监控.

5.2.3 SaaS 层的安全

数据安全和软件安全是 SaaS 层安全的两个最重要的问题.

数据安全就是给用户提供数据的可感知性、完整性、可用性、安全性和可控性. 这一领域是目前云安全领域论文最多的一个领域. 其主要技术手段是采用密码技术和纠错编码技术 [85~88,146~149].

密码的应用不能没有密钥管理. 传统密钥协商协议, 如 DH 密钥协商协议等, 都要求双方进行同样的计算. 可是对于云计算来说, 云平台拥有巨大的计算能力, 而云终端的计算能力是有限的, 两者的计算能力存在巨大的非对称. 因此, 传统的密钥协商协议对于云计算系统是不适用的. 文献 [244] 给出了一种非对称密钥协商协议. 让云平台承担大的计算量, 让云终端承担小的计算量, 双方经过不同的计算, 却得到相同的密钥.

软件安全是信息安全中一个困难问题. 确保软件安全主要有以下方法: 第 1 个是编写安全代码, 这是主动的方法, 但是我们很难确保完全做好这一点. 第 2 个是对软件进行安全测试, 以发现并修复软件的安全缺陷. 第 3 个是对软件的运行实施安全监控. 请参见 5.3 小节.

我国在可信云计算领域已经发展到产业化阶段. 武汉大学与华为公司合作开发出我国第一款可信云服务器, 其主要可信技术特征有: 支持中国 TCM/TPM 2.0 芯片、支持中国商用密码算法、可信启动 (TBOOT)、从 BIOS 到 VM 的信任度量、支持 TXT 多次度量技术、支持虚拟机环境下的软件安全保护、支持云系统的可信管理.

这款可信云服务器被配置到华为的 FusionCloud 系统中, 并被用于可信电信云 (NFV)、华为可信计算池 (TCP) 等应用中. 华为公司在可信云服务器获得实际好处后, 更进一步开发出可信路由器等可信网络产品, 在我国首先闯出一条网络产品可信化的网络安全之路.

武汉大学还与浪潮公司合作开发出可信云服务器, 并用于浪潮可信云系统中.

华为公司和浪潮公司的可信云服务器的应用实践表明, 可信计算技术对于确保云服务器的资源完整性、虚拟化环境的安全性、数据的安全存储、对抗恶意软件入侵等方面都发挥了重要的作用.

必须指出, 可信计算并不排斥其他信息安全技术, 相反地把其他信息安全技术与可信计算整合起来, 将会得到更好的安全性.

确保云计算安全是一个复杂的系统工程, 尽管目前人们采用了各种信息安全措施, 但是离人们对云计算安全的期望还有很大距离. 可以相信, 人们将会坚持不懈地朝期望目标前进.

5.3 软件安全

软件 (或程序) 行为是指软件运行时表现出的状态演变过程, 可以从底层的二进制指令到高层的程序语句、函数、系统调用等不同层次刻画软件行为. 软件的行为模型就是指根据某一层次的行为信息而构建的行为状态序列以及状态变迁. 它可以表征软件的正常行为, 并用于软件行为的异常检测. 但是, 源于软件自身存在的缺陷和软件运行环境的不可信, 软件在黑客攻击或者在不可信环境下会偏离其预期的行为, 产生不可预料的后果. 软件安全就是确保软件行为在软件的生命周期中都是预期的. 文献 [245] 从软件静态分析和动态分析角度剖析了软件的结构和行为. 文献 [246] 从软件状态、软件确保服务、软件确保措施及时间 4 个维度构建了软件确保模型.

5.3.1 软件安全威胁

软件安全威胁包括拒绝服务、隐私泄漏、权限提升、恶意代码执行、功能误用等. 拒绝服务攻击以耗尽系统的资源实施攻击, 如耗尽 CPU、内存、网络带宽、电源等资源. 隐私泄漏在社交网络和移动设备中极为普遍. 另外, 利用侧信道攻击也可以推测出用户的敏感信息, 如从击键产生的振动可推测用户的按键输入、当前的活动窗口、敏感输入信息 [247,248] 以及移动轨迹 [249]. 权限提升可以给攻击代码获得更高的权限, 如获得 Root 权限. 如果攻击者的组件优于合法组件, 则会产生组件劫持, 造成权限提升 [250]. 恶意代码执行是危害最大的一种攻击, 此时攻击者可以植入任何想要执行的代码, 包括常见的 Shellcode、木马或蠕虫等, 从而劫持软件的正常执行流程. 功能误用是指攻击者可以随意调用限制使用的开放 API 函数, 如浏览器插件的开放等 [251].

5.3.2 软件安全威胁的防御

根据容错的原理, N 版本软件技术通过软件冗余可达到软件容错的目的, 因而可以抵抗某些攻击. 文献 [252] 利用改变指令或者数据的位置和顺序, 使程序多样化, 实现了缓冲区溢出攻击的检测. 常见的多样性安全防御技术包括地址随机化、数据随机化、指令随机化、接口随机化等. 应当指出, 多版本软件技术可以增加可靠性和安全性, 但也会增加开发和维护成本.

软件的安全检测是防御软件安全威胁的重要方法. Shellcode 生命周期包括传输、加载和执行 3 个阶段, 因此, shellcode 的防御和检测也可从 3 个阶段进行.

在网络流中检测网络流是否包含 shellcode 的特定代码和指令, 可以在传输阶段发现并阻塞 shellcode. 基于签名的检测方法用于 shellcode 加载前的检测. 如果 shellcode 使用 ROP 编程, 则基于签名的检测方法失效. 基于完整性的检测方法应用于 shellcode 执行前. Shellcode 的执行会导致程序指针偏离正常轨迹, 进入非法代码区域. 如果建立合法的 PC (program pointer) 跳转表, 则可以检测出 Shellcode. 基于行为的检测方法可应用于 shellcode 执行中的检测, 如捕获异常的系统 API 调用等检

测. 文献 [253] 可以识别用户动作的位置和特定对话框, 实现用户意图与文件关联, 从而检测 shellcode 的下载行为. 文献 [251] 根据用户的浏览行为检测 shellcode 的下载行为. 另外, 基于漏洞利用模式的检测方式则把对 shellcode 的检测转移到对某种漏洞利用模式上, 如 HeapSpray 和 HeapLib 会在短时间内分配大量堆内存、有比较固定的 EIP 跳转地址. 文献 [254] 利用漏洞模式检测模块之间的通信达到检测 shellcode 的目的. 该检测方法依赖于漏洞模式, 针对性比较强.

针对 APT 的攻击, 不仅需要从软件的全生命周期通盘考虑程序的安全性, 如微软的 SDL 从需求、设计、编码、测试、运行和维护等考虑安全性, 而且需要考虑程序的运行环境的安全确保, 包括程序调用的公共库安全确保、内核库的安全确保.

5.3.3 今后的研究

(a) 设计安全实用的软件安全确保方案, 包括高效的细粒度的随机化方案; 将安全防御从自身行为的审查扩展到 shellcode 的检测、高级木马检测等方面.

(b) 设计便于标记代码/地址/数据随机化、内存对象资源的访问控制和内存对象的加密混淆的程序设计语言, 程序利用携带的这些标记便于与操作系统、安全软件实现协同防御.

(c) 针对 X86 指令系统损失变量类型信息, 设计准确识别二进制程序中数据结构的方法, 在二进制层还原高级程序语言的语义信息, 构建精确、细粒度的软件行为轮廓.

(d) 结合控制流分析、数据流分析、切片分析、代码插桩等技术, 实现灵活的、功能丰富的漏洞挖掘平台.

5.4 嵌入式系统安全

5.4.1 工业控制系统安全

2010 年, 黑客利用 APT 攻击, 成功攻击了伊朗的核工厂, 损坏了 70% 以上的铀浓缩离心机, 重创了伊朗的核计划. 这一事件标志着, 黑客攻击从传统的软打击, 上升为直接毁坏硬件设备的硬摧毁, 从而敲响了工控系统防范攻击的警钟. 在这一攻击过程中, Stuxnet 病毒发挥了核心作用, 因此, 如何防范 Stuxnet 类病毒的攻击, 成为工业控制系统安全的一个核心问题.

工业控制系统直接关系到国家安全和国计民生, 因此确保我国工业控制系统安全成一项刻不容缓的战略任务.

将可信计算技术用于工业控制系统是提高其可信性的有效措施 [1,2,4,225,226]. 但是工业控制系统与普通计算机系统相比有自己的特殊性, 不考虑这些问题是不行的.

(a) 工业控制系统不仅对安全性要求很高, 对可靠性要求更高.

(b) 多数工业控制系统对适时性要求高, 因此任何安全措施必须满足其对适时性的要求.

(c) 许多工业控制系统具有一旦开机久长期不关机的特点. 这就对可信计算提出了可多次度量的要求, 像可信 PC 机那样开机度量一次的方式是不适用的.

5.4.2 TrustZone

TrustZone 是 ARM 为了构建系统的可信执行环境 TEE, 所采用的一种安全保护技术 [255]. TrustZone 的整体安全思想是通过系统结构将其软硬件资源划分为相互隔离的两个区域: 安全区和普通区. 每个区的工作模式都包含用户模式和特权模式. ARM 通过其总线系统确保安全区的资源不被普通区

所访问. 非安全区的软件只能访问非安全区的资源, 而安全区的软件能访问所有资源. 在安全区中还有一个监控模式. 这个监控模式分别与两区的特权模式相连. 设置监控模式是为了实现两区间的切换.

当普通区的用户模式需要获取安全区的服务时, 首先需要进入到普通区的特权模式, 在该模式下执行安全监控调用指令, 处理器将进入到监控模式, 监控模式备份普通区的上下文, 然后进入到安全区的特权模式, 此时的运行环境是安全区的执行环境, 此后进入到安全区的用户模式, 得到相应的安全服务.

ARM 上电后首先是 ROM 中的 Bootloader 初始化关键的外设, 随后切换到 Flash 存储器中的 Bootloader, 然后启动安全区的 OS. 之后才启动普通区的 Bootloader 去装载普通区的 OS. 至此系统启动完成. 启动过程中的软件认证采用了基于 RSA 密码的签名认证协议. 此外, 在启动过程中后装入的组件必须要能通过前面装入的组件的认证, 从而构成了信任链. 可见, ROM 中的 Bootloader 是信任根. 由此可知, TrustZone 采用了可信计算机制.

从目前的研究来看, TrustZone 总体上是安全的. 文献 [256] 发现 TrustZone 存在整数溢出缺陷.

今后值得研究的问题有: 第一, 目前对 TrustZone 的安全性分析是不够的, 需要深入研究. TrustZone 的安全性主要是依靠总线的访问控制, 因此应当对此进行重点研究. 第二, 虽然 TrustZone 的启动过程采用了可信计算的信任链技术, 但是缺少 TPM 等可信计算技术. 因此, 应当研究 TrustZone 与 TPM 等可信计算技术相结合的问题. 第三, TrustZone 的实际应用尚少, 应加大应用研究, 在应用中发现问题并解决问题.

6 信息内容安全

在全球信息化的今天, 互联网将朝着开放性、异构性、移动性、动态性的方向发展. 通过不断演化, 将产生下一代互联网、5G 移动通信网络、移动互联网、物联网等新型网络形式以及云计算等服务模式. 同时, 随着工业 4. 0 影响全球和我国实施 “互联网 +” 行动, 互联网与传统行业深度融合也是大势所趋. 互联网及其延伸的新业态为人们在生活和生产中获取信息、互相交流、协同工作带来了巨大便利, 并直接促进了相关行业的转型升级. 但是, 互联网也带来了一些负面影响, 色情、反动等不良信息在网络上大量传播, 垃圾电子邮件等不正当行为的泛滥, 利用网络传播电影、音乐、软件的侵犯版权行为, 甚至通过网络钓鱼方式欺诈用户以及网络暴力和网络恐怖主义活动等问题, 这些行为完全背离了互联网设计者的初衷, 也不符合广大网络用户的利益. 因此, 在建设信息化社会过程中, 提高信息安全保障水平, 提高对互联网各种不良信息的监控能力, 是国家信息化建设的重要一环.

信息内容安全技术是研究利用计算机从包含海量信息并且迅速变化的网络中, 对特定安全主题相关信息进行自动获取、识别和分析的技术. 根据它所处的网络环境, 也称为网络内容安全. 信息内容安全是管理信息传播的重要手段, 属于网络安全系统的核心理论与关键组成部分, 对提高网络使用效率, 净化网络空间, 保障社会稳定具有重要意义.

大力推进信息化是我国现代化建设的战略举措, 也是贯彻落实科学发展观、全面建设小康社会和建设创新型国家的迫切需要和必然选择. 信息内容安全作为网络安全中智能信息处理的核心技术, 为先进网络文化建设, 加强社会主义先进文化的网上传播提供了技术支撑, 属于国家信息安全保障体系的重要组成部分. 因此, 信息内容安全研究不仅具有重要的学术意义, 也具有重要的社会意义.

6.1 信息内容安全威胁

在互联网、电信网、电视网等各类网络信息共享环境中, 内容安全所面临的威胁有泄露、欺骗、破坏和篡夺 [257~261]. 其具体情况如下: (1) 网络中有大量公开的信息, 例如某人的姓名、工作单位、电子邮箱、电话号码等. 由于这些公开信息的获取成本非常低, 在某些情况下, 这些信息会被整合, 并可能会被滥用, 例如某些公司会将这些数据作为商业信息出售, 还有些诈骗集团会利用这些信息进行诈骗. 所以网络上的信息泄露还可以指将特定信息向特定人或组织进行传播, 以妨碍特定人或组织的正常生活或工作. (2) 其次, 网络的开放性和自主性导致信息由各个组织自主发布并共享到网络中. 这带来了很多欺骗的威胁. 网络的地址和网站的内容都存在伪造的可能. 这些是网络中无法保证信息完整性 (尤其是信息来源) 造成的. (3) 信息还会被非法地传播. 在很多网络中被发现具有知识产权的音乐和电影被广泛地传播, 侵犯了别人的知识产权. (4) 信息在传播过程中也可能被篡改. 篡改信息的目的可能是消除信息的来源信息, 使之无法跟踪. 也可能是伪造信息的内容. 此外, 信息篡改后还可能携带病毒或者木马, 这将严重危害计算机信息系统的安全.

6.2 网络信息内容获取

6.2.1 网络媒体信息获取流程

与面向特定点的网络通讯信息获取不同, 网络媒体信息获取环节的工作范围理论上可以是整个国际互联网. 传统的网络媒体信息获取环节从预先设定的, 包含一定数量 URL 的初始网络地址集合出发, 首先获取初始集合中每个网络地址对应的发布内容. 网络媒体信息获取环节一方面将初始网络地址发布信息主体内容按照系列内容判重机制, 有选择地存入互联网信息库 [262~264].

另一方面, 网络媒体信息获取环节还进一步提取已获取信息内嵌的超链接网络地址, 并将所有超链接网络地址置入待获取地址队列, 以 “先入先出” 方式逐一提取队列中的每个网络地址发布信息. 网络媒体信息获取环节循环开展待获取队列中的网络地址发布信息获取 [265]、已获取信息主体内容提取 [266,267]、判重与信息存储 [268~270], 以及已获取信息内嵌网络地址提取并存入待获取地址队列操作, 直至遍历所需的互联网络范围.

理想的网络媒体信息获取流程主要由初始 URL 集合 —— 信息 “种子” 集合, 等待获取的 URL 队列、信息获取模块、信息解析模块、信息判重模块与互联网信息库共同组成.

6.2.2 网络媒体获取的典型工具

网络爬虫是在互联网上实施信息内容获取的主要工具. 网络爬虫是一种按照一定的规则, 自动地抓取互联网信息的程序或者脚本. 互联网上的信息发布是分散的和独立的, 但信息间又是相互连接的 [271~274]. 爬虫就在超链接所建立的网上穿梭, 这是爬虫又被称为蜘蛛的原因.

互联网信息资源非常庞大, 在有限的网络资源的条件下, 网络蜘蛛必须有选择性. 针对不同的服务对象, 网络爬虫的行为大体分为两类. 一类是服务于搜索引擎等搜索类应用的网络爬虫, 它的信息抓取规则是尽可能地覆盖更多的互联网网站, 单一网站内的搜索深度要求不高. 另一类是针对性进行信息收集的应用中, 例如舆情分析系统则要求它的网络爬虫具备高搜索深度和一定的主题选择能力. 具有高搜索深度的爬虫被称为路径追溯爬虫, 该类爬虫深入地尽可能抓取给定网站的全部资源. 具有主题选择能力的爬虫被称为主题爬虫, 该类爬虫会判断抓取的资源是否属于用户指定的主题, 并持续对有关给定主题的网页进行搜索和抓取.

网络爬虫通常采用分布式机制来保证信息获取的全面性和时效性. 由于互联网资源规模巨大, 而下载需要时间, 所以网络爬虫都采用多进程或者多线程, 甚至是分布式方式同时下载多个网络资源 (文本、图片、音频或者视频等), 也就是说这是一项群体作业, 爬虫们 (下载器) 集体一起完成抓取的任务 (也就是为什么网络爬虫也被称为蚂蚁的原因). 网络爬虫还需要避免过于频繁获取信息而被媒体网站判为 “恶意”. 一方面可以通过适当选择周期遍历时间间隔, 防止信息获取行为造成网络媒体负载过重; 另一方面则涉及到定期修改用于内容获取的网络客户端信息请求内容 (内容协商行为), 避免遭遇目标网络媒体的拒绝服务.

6.3 信息内容特征抽取和选择

信息内容的表示及其特征项的选取是数据挖掘、信息检索的一个基本问题, 它把从信息中抽取出的特征词进行量化来表示文本信息. 将它们从一个无结构的原始信息内容转化为结构化的计算机可以识别处理的信息, 即对信息内容进行科学地抽象, 建立它的数学模型, 用以描述和代替信息内容. 使计算机能够通过对这种模型的计算和操作来实现对信息内容的识别.

对文本信息内容而言, 由于文本是非结构化的数据, 要想从大量的文本中挖掘有用的信息就必须首先将文本转化为可处理的结构化形式. 文本特征选择对文本内容的过滤和分类、聚类处理、自动摘要以及用户兴趣模式发现、知识发现等有关方面的研究都有非常重要的影响. 通常根据某个特征评估函数计算各个特征的评分值, 然后按评分值对这些特征进行排序, 选取若干个评分值最高的作为特征词, 这就是特征选择 [275,276]. 特征选择已经有了很多成熟的方法, 绝大多数都是基于统计的. 信噪比方法源于信号处理领域, 表示信号强度与背景噪声的差值. 如果将特征项作为一个信号来看待, 那么特征项的信噪比可以作为该特征项对文本类别区分能力的体现. 信息增益是机器学习领域, 尤其是构建决策树分类器时常采用的特征选择方法, 信息增益也利用到信息熵的概念, 依据特征项与类别标签之间的统计关系作为评价指标. 卡方统计的判断依据是特征项与类别标签的相关程度, 即认为一个特征项与某个类别如果满足同时出现的情况, 则说明该特征项能比较好地代表该类别. 当单纯的特征选择无法满足信息表示的要求时, 需要进行特征重构. 特征重构以特征项集合为输入, 利用对特征项的组合或转换生成新的特征集合作为输出.

对于音频信息内容, 充分地分析和提取其物理特征 (例如频谱等)、听觉特征 (例如响度、音色等) 和语义特征 (例如语音的关键词、音乐的旋律节奏等), 有效地实现音频信息的内容分类和检索至关重要 [277~279]. 根据检索对象和检索方法的不同, 国内外在音频检索方面的研究大体分为语音检索、音乐内容检索和音乐例子检索几类. 音频检索第一步是建立数据库, 对音频数据进行特征提取, 并通过特征对数据聚类. 然后检索引擎对特征向量与聚类参数集匹配, 按相关性排序后通过查询接口返回给用户. 音频信号的特征抽取指提取音频的时域和频域特征, 将不同内容的音频数据予以区分. 因此, 所选取的特征应该能够充分地反映音频的物理和听觉特征, 对环境的改变具有较好的鲁棒性. 在进行音频特征抽取时, 通常将音频划分为等长的片段, 在每个片段内有划分帧. 这样, 特征抽取所采用的特征包括基于帧的特征和基于片段的特征两种.

此外, 相比文本信息而言, 数字图像具有信息量大、像素点之间的关联性强等特点. 因此, 对于数字图像的处理方法与文本处理方法有较大的差别. 图像的特征抽取盒选择主要包含以下几个方面:

(1) 图像颜色特征提取 [280]. 所谓图像的颜色特征, 通俗地说, 即能够用来表示图像颜色分布特点的特征向量. 常见的颜色特征有颜色直方图、颜色聚合矢量、颜色矩等等.

(2) 图像纹理特征提取 [281]. 能够用来表示图像纹理 (亮度变化) 特点的特征向量. 纹理信息是亮度信息和空间信息的结合体, 反映了图像的亮度变化情况. 常见的纹理特征有灰度共生矩阵、Gabor

小波特征、Tamura 纹理特征等等.

(3) 其他图像特征 [282,283]. 除了以上两种常用的图像特征 (颜色特征和纹理特征), 现有的图像分类、检索系统中还使用边缘特征和轮廓特征.

6.4 信息内容分析和处理

海量信息内容分析的基本处理环节可以归结为匹配、分类和过滤. 其他更加复杂的处理问题则是上述简单处理问题的组合. 在信息检索和文本编辑等等应用中, 快速对用户定义的模式或者短语进行匹配是最常见的需求. 在文本信息过滤的处理中, 匹配算法也一直是人们所关注的. 一个高效的匹配算法会使信息处理变得迅速而准确, 从而得到使用者的认可; 反之, 会使处理过程变得冗长而模糊, 让人难以忍受.

6.4.1 信息内容分类

分类算法在图像分类、索引和内容理解方面都有直接的应用, 其主要功能是: 通过分析不同图像类别、各种图像特征之间存在的差异, 将其按内容分成若干类别 [284,285]. 经过几十年的研究与实践, 目前已经有数十种的分类方法. 任何分类器构建都可以抽象为一个学习的过程, 而学习又分为监督学习和非监督学习两种.

6.4.2 信息过滤

信息过滤是大规模内容处理的一种典型操作, 它是对陆续到达的信息进行过滤操作, 可以认为是满足用户信息需求的信息选择过程, 将符合用户需求的信息保留, 将不符合用户需求的信息过滤掉 [286].

Hanani 等 [287] 从另一个角度给出了信息过滤的另一个定义: 信息过滤是指从动态的信息流中将满足用户兴趣的信息挑选出来, 用户的兴趣一般在较长一段时间内不会改变 (静态). 信息过滤通常是在输入数据流中移除数据, 而不是在输入数据流中找到数据.

实际上, 在内容安全领域, 信息过滤是提供信息的有效流动, 消除或者减少信息过量、信息混乱、信息滥用造成的危害, 但在目前的研究阶段看, 仍然处于较为初级的研究阶段, 为用户剔除不合适的信息是当前内容安全领域信息过滤的主要任务之一. 信息过滤技术有很多种不同的分类方法: 按照主动性分, 可以分为主动信息过滤和被动信息过滤; 按照过滤器所在位置, 可以分为在信息的源头、在服务器上和在客户端过滤; 按照过滤的方法, 可以分为基于内容的过滤、基于用户兴趣的过滤和协同过滤. 根据获得知识的方法, 可以分为显式的方式和隐含的方式. 信息过滤可以被应用到很多方面, 比如 Internet 搜索结果的过滤、用户电子邮件过滤、服务器/新闻组过滤、浏览器过滤、用户爱好推荐.

6.5 网络舆情监测与预警

网络舆情预警监测系统主要完成互联网海量信息资源的综合分析, 提取支持政府部门决策所需的有效信息 [288]. 目前, 国内外政府职能部门与研究机构, 尤其是西方发达国家, 针对该类系统应用与技术研发投入了相当的资源, 使该类系统与技术得到了全面发展 [289]. 各国对于通过互联网捕获与掌握各类政治、军事、文化信息都从战略角度予以高度重视. 以美国为例, 为提高政府对于信息的掌控能力, 任命了 John Negroponte 为首任国家情报局长, 重点解决多渠道信息的融合和统一表达, 提高信息控制能力.

网络舆情监测技术的发展趋势可以归结为以下几个方面:

1) 针对信息源的深入信息采集. 传统搜索引擎中的 Robot, 一般采用广度优先的策略来遍历 Web 并下载文档. 系统中维护一个超链队列 (或者堆栈) 包含一些起始 URL. Robot 从这些 URL 出发, 下载相应的页面, 把抽取到的新超链加入到队列 (或者堆栈) 中. 上述过程不断递归重复, 直到队列 (或者堆栈) 为空. 而以 Google、Hotbot、百度等为代表的搜索引擎技术, 即俗称 "大搜索" 的技术, 并不能完全满足本项目中网络舆情预警监测系统的需求. 具体而言, "大搜索" 技术主要不足体现在对于互联网定点信息源信息的提取率 (一般定义为指定时刻提取信息比特数/信息源信息总比特数) 过低.

2) 异构信息的融合分析. 互联网信息的一大特征就是高度的异构化. 所谓异构化, 指的是互联网信息在编码、数据格式以及结构组成方面都存在巨大的差异. 而对于海量信息分析与提取的重要前提就是对不同结构的信息可以在统一表达或标准的前提下进行有机的整合, 并得出有价值的综合分析结果. 对于异构信息的融合分析, 目前比较流行的方式可以分为两类. 一是通过采取通用的具有高度扩展性的数据格式进行资源的整合, 如 XML (extensible markup language). 二是采取基于语义等应用层上层信息的抽象融合分析, 如 RDF (resource description framework).

3) 非结构信息的结构化表达. 与传统的信息分析系统处理对象不同, 针对互联网信息分析处理的大量对象是非结构化信息. 非结构化信息的特点对于阅读者而言比较容易理解, 然而对于计算机信息系统处理却相当困难. 对于结构化数据, 长期以来通过统计学家、人工智能专家和计算机系统专家的共同努力, 有相当优秀的技术与方法可以提供相当准确而有效的分析.

伴随互联网的迅速普及, 各式各样、良莠不齐的发布内容日渐泛滥, 传统、纯粹的 "人海" 战术已经无法满足当前互联网媒体信息监控工作的实际需求. 基于互联网媒体发布内容主动获取、分析挖掘与表达呈现等系列技术开展互联网论坛监测工作, 首先需要保证相关监测产品对于目标站点发布数据的提取比率, 即监测产品信息提取部分的具体性能. 根据当前网络监管部门对于互联网论坛监控工作的实际应用需求, 成熟的互联网论坛监控产品必须具备针对指定信息源的深度挖掘技术. 其次, 当前互联网利用动态脚本生成的动态内容已经占据主导地位, 出于功能全面性与产品实用性等多方考虑, 面向结构迥异、风格多样的数据发布源实施互联网媒体信息监控工作, 相关监控产品信息提取部分还需具备相当高的普适性与可扩展性.

6.6 网络信息内容综合管控

网络管理技术就是监督、组织和控制网络通信服务以及信息处理所必需的各种技术手段和措施的总称. 其目标是确保计算机网络的持续正常运行, 并在计算机网络运行出现异常时能及时响应和排除故障. 为了系统性地保障信息内容安全, 实现网络信息内容综合管控也势在必行 [290].

在网络应用的深入和技术频繁升级的同时, 非法访问、恶意攻击等安全威胁也在不断推陈出新, 愈演愈烈. 防火墙、VPN、IDS、防病毒、身份认证、数据加密、安全审计等安全防护和管理系统在网络中得到了广泛应用. 虽然这些安全产品能够在特定方面发挥一定的作用, 但是这些产品大部分功能分散, 各自为战, 形成了相互没有关联的、隔离的 "安全孤岛"; 各种安全产品彼此之间没有有效地统一管理调度机制, 不能互相支撑、协同工作, 从而使安全产品的应用效能无法得到充分地发挥. 从信息内容安全管理的角度来说, 最直接的需求就是在一个统一的界面中监视网络中各种安全设备的运行状态, 对产生的大量日志信息和报警信息进行统一汇总、分析和审计; 同时在一个界面完成安全产品的升级、攻击事件报警、响应等功能.

另外, 对大型网络而言, 与信息内容管理相关的事件变得越来越复杂, 网络管理员必须将各个信息内容管控设备、系统产生的事件、信息关联起来进行分析, 才能发现新的或更深层次的信息内容安

全问题. 因此, 用户的网络管理需要建立一种新型的整体网络信息安全管理解决方案 —— 网络信息内容安全综合管控平台, 来总体配置、调控整个网络多层面、分布式的安全系统, 实现对网络中各种信息内容安全资源的集中监控、统一策略管理、智能审计及多种安全功能模块之间的互动, 从而有效简化网络信息内容安全管理工作, 提升信息内容安全水平和可控制性、可管理性, 降低用户的整体信息内容安全管理开销.

致谢 本文的写作得到傅建明、张立强、袁巍、习宁、卢笛、伍军的帮助, 在此向他们表示感谢!

参考文献

1 沈昌祥, 张焕国, 冯登国, 等. 信息安全综述. 中国科学 E 辑: 信息科学, 2007, 37: 129–150
2 Shen C X, Zhang H G, Feng D G, et al. Survey of information security. Sci China Ser F-Inf Sci, 2007, 50: 273–298
3 Zhang H G, Qin Z P. Introduction to Evolution Cryptology. Wuhan: Wuhan University Press, 2010 [张焕国, 覃中平. 演化密码引论. 武汉: 武汉大学出版社, 2010]
4 Zhang H G, Zhao B. Trusted Computing. Wuhan: Wuhan University Press, 2011 [张焕国, 赵波. 可信计算. 武汉: 武汉大学出版社, 2011]
5 Daniel J B, Johannes B, Erik. Post Quantum Cryptology. Beijing: Tsinghua University Press, 2015 [张焕国, 王后珍, 杨昌, 等. 抗量子计算密码. 北京: 清华大学出版社, 2015]
6 Zhang H G, Guan H M, Wang H Z. Current research of post quantum cryptography. In: Cryptography Development Report of China. Beijing: Electronics Industry Press, 2011. 1–31 [张焕国, 管海明, 王后珍. 抗量子密码体制的研究现状. 见: 中国密码学发展报告. 北京: 电子工业出版社, 2011. 1–31]
7 Information Security Professional Instruction Committee-Information Security Professional Specification Project Group. Information Security Majority Insructive Specification. Beijing: Tsinghua University Press, 2014 [信息安全类专业教学指导委员会信息安全专业规范项目组. 信息安全专业指导性专业规范. 北京: 清华大学出版社, 2014]
8 Zhang H G, Du R Y, Fu J M, et al. Information security discipline. Netw Secur, 2014, 56: 619–620 [张焕国, 杜瑞颖, 傅建明, 等. 论信息安全学科. 网络安全, 2014, 56: 619–620]
9 Zhang H G, Wang L N, Du R Y, et al. Information security discipline system structure research. J Wuhan Univ, 2010, 56: 614–620 [张焕国, 王丽娜, 杜瑞颖, 等. 信息安全学科体系结构研究. 武汉大学学报理学版, 2010, 56: 614–620]
10 Bar-On A, Dinur I, Dunkelman O, et al. Cryptanalysis of SP networks with partial non-linear layers. In: Advances in Cryptology EUROCRYPT. Berlin: Springer, 2015. 315–342
11 Sun S W, Hu L, Wang P, et al. Automatic security evaluation and (related-key) differential characteristic search: application to SIMON, PRESENT, LBlock, DES(L) and other bit-oriented block ciphers. In: Advances in Cryptology ASIACRYPT. Berlin: Springer, 2014. 158–178
12 Emami S, Ling S, Nikoli04 I, et al. Low probability differentials and the cryptanalysis of full-round CLEFIA-128. In: Advances in Cryptology ASIACRYPT. Berlin: Springer, 2014. 141–157
13 Bogdanov A, Knudsen L R, Leander G, et al. PRESENT: an ultra-lightweight block cipher. In: Cryptographic Hardware and Embedded Systems-CHES. Berlin: Springer, 2007. 450–466
14 Wu W L, Zhang L. LBlock: a lightweight block cipher. In: Applied Cryptography and Network Security. Berlin: Springer, 2011. 327–344
15 Borghoff J, Canteaut A, Güneysu T, et al. PRINCE-a low-latency block cipher for pervasive computing applications. In: Advances in Cryptology ASIACRYPT. Berlin: Springer, 2012. 208–225
16 Albrecht M R, Benedikt D, Kavun E B, et al. Block ciphers-focus on the linear layer (feat. PRIDE). In: Advances in Cryptology CRYPTO. Berlin: Springer, 2014. 57–76
17 Gilbert H. A simplified representation of AES. In: Advances in Cryptology ASIACRYPT. Berlin: Springer, 2014. 200–222
18 Papakonstantinou P A, Yang G. Cryptography with streaming algorithms. In: Advances in Cryptology CRYPTO. Berlin: Springer, 2014. 55–70
19 Banegas G. Attacks in stream ciphers: a survey. http://eprint.iacr.org/2014/677.pdf
20 Àgren M, Löndahl C, Hell M, et al. A survey on fast correlation attacks. Cryptogr Commun, 2012, 4: 173–202
21 Hell M, Johansson T, Brynielsson L. An overview of distinguishing attacks on stream ciphers. cryptogr commun, 2009, 1: 71–94
22 Knellwolf S, Meier W. High order differential attacks on stream ciphers. Cryptogr Commun, 2012, 4: 203–215
23 Dinur I, Shamir A. Applying cube attacks to stream ciphers in realistic scenarios. Cryptogr Commun, 2012, 4: 217–232

24 Zhang J M, Qi W F, Tian T, et al. Further results on the decomposition of an NFSR into the cascade connection of an NFSR into an LFSR. IEEE Trans Inf Theory, 2015, 61: 645–654
25 Yang D, Qi W F, Zheng Q X. Further results on the distinctness of modulo 2 reductions of primitive sequences over $Z/(2^{32-1})$. Design Code Cryptogr, 2015, 74: 467–480
26 ETSI/SAGE TS 35.222-2011. Specification of the 3GPP Confidentiality and Integrity Algorithms 128-EEA3 and 128-EIA3. Document 2: ZUC Specification
27 Wang X Y, Yu H B, Yin Y L. Efficient collision search attacks on SHA-0. In: Advances in Cryptology-CRYPTO. Berlin: Springer, 2005. 1–16
28 Wang X Y, Yin Y L, Yu H B. Finding collisions in the full SHA-1. In: Advances in Cryptology-CRYPTO. Berlin: Springer, 2005. 17–36
29 Wang X Y, Lai X J, Feng D G, et al. Cryptanalysis of the hash functions MD4 and RIPEMD. In: Advances in Cryptology EUROCRYPT. Berlin: Springer, 2005. 1–18
30 Wang X Y, Yu H B. How to break MD5 and other hash functions. In: Advances in Cryptology EUROCRYPT, Berlin: Springer, 2005. 19–35
31 Jian G, Peyrin T, Yu S, et al. Updates on generic attacks against HMAC and NMAC. In: Advances in Cryptology-CRYPTO. Berlin: Springer, 2014. 131–148
32 Guo J, Sasaki Y, Wang L, et al. Cryptanalysis of HMAC/NMAC-Whirlpool. In: Advances in Cryptology-ASIACRYPT. Berlin: Springer, 2013. 21–40
33 Leurent G, Peyrin T, Wang L. New generic attacks against hash-based MACs. In: Advances in Cryptology-ASIACRYPT. Berlin: Springer, 2013. 1–20
34 Peyrin T, Yu S, Lei W. Generic related-key attacks for HMAC. In: Advances in Cryptology-ASIACRYPT. Berlin: Springer, 2012. 580–597
35 Catalano D, Fiore D. Practical homomorphic MACs for arithmetic circuits. In: Advances in Cryptology-EUROCRYPT. Berlin: Springer, 2013. 336–352
36 Cryptographic competitions, http://competitions.cr.yp.to/index.html
37 Bogdanov A, Mendel F, Regazzoni F, et al. ALE: AES-based lightweight authenticated encryption. In: Fast Software Encryption. Berlin: Springer, 2014. 447–466
38 Bilgin B, Bogdanov A, Knežević M, et al. Fides: lightweight authenticated cipher with side-channel resistance for constrained hardware. In: Cryptographic Hardware and Embedded Systems-CHES. Berlin: Springer, 2013. 142–158
39 Hoang V T, Krovetz T, Rogaway P. Robust authenticated-encryption AEZ and the problem that it solves. In: Advances in Cryptology-EUROCRYPT. Berlin: Springer, 2015. 15–44
40 Sarkar P. Modes of operations for encryption and authentication using stream ciphers supporting an initialisation vector. Cryptogr Commun, 2014, 6: 189-231
41 Lu X H, Li B, Jia D D. KDM-CCA security from RKA secure authenticated encryption. In: Advances in Cryptology-EUROCRYPT. Berlin: Springer, 2015. 559–583
42 Joo C H, Yun A. Homomorphic authenticated encryption secure against chosen-ciphertext attack. In: Advances in Cryptology-ASIACRYPT. Berlin: Springer, 2014. 173–192
43 Andreeva E, Bogdanov A, Luykx A, et al. How to securely release unverified plaintext in authenticated encryption. In: Advances in Cryptology-ASIACRYPT. Berlin: Springer, 2014. 105–125
44 Wu S, Wu H, Huang T, et al. Leaked-state-forgery attack against the authenticated encryption algorithm ALE. In: Advances in Cryptology-ASIACRYPT. Berlin: Springer, 2013. 377–404
45 Dinur I, Jean J. Cryptanalysis of FIDES. In: Fast Software Encryption. Berlin: Springer, 2014. 224–240
46 Nandi M. Forging attacks on two authenticated encryption schemes COBRA and POET. In: Advances in Cryptology-ASIACRYPT. Berlin: Springer, 2014. 126–140
47 Wang P, Wu W L, Zhang L T. Cryptanalysis of the OKH authenticated encryption scheme. In: Information Security Practice and Experience. Berlin: Springer, 2013. 353–360
48 Shamir A. Identity-based cryptosystems and signature schemes. In: Proceedings of CRYPTO 84 on Advances in Cryptology. Berlin: Springer, 1985. 47–53
49 Boneh D, Franklin F. Identity-based encryption from the Wail pairing. In: Advances in Cryptology CRYPTO. Berlin: Springer, 2001, 32: 586–615
50 Dan B, Boyen X, Goh E J. Hierarchical identity based encryption with constant size ciphertext. In: Advances in Cryptology EUROCRYPT. Berlin: Springer, 2005. 440–456
51 Waters B. Efficient identity-based encryption without random oracles. In: Advances in Cryptology EUROCRYPT. Berlin: Springer, 2005. 114–127
52 Ducas L, Lyubashevsky V, Prest T. Efficient identity-based encryption over NTRU lattices. In: Advances in Cryptology ASIACRYPT. Berlin: Springer, 2014. 22–41
53 Blazy O, Kiltz E, Pan J. (Hierarchical) Identity-based encryption from affine message authentication. In: Advances in Cryptology CRYPTO. Berlin: Springer, 2014. 408–425
54 Al-Riyami S S, Paterson K G. Certificateless public key cryptography. In: Advances in Cryptology ASIACRYPT.

Berlin: Springer, 2003. 452–473
55 Dan B, Gentry C, Waters B. Collusion resistant broadcast encryption with short ciphertexts and private keys. In: Advances in Cryptology CRYPTO. Berlin: Springer, 2005. 258–275
56 Dan B, Waters B, Zhandry M. Low overhead broadcast encryption from multilinear maps. In: Advances in Cryptology CRYPTO. Berlin: Springer, 2014. 206–223
57 Sahai A, Waters B. Fuzzy identity-based encryption. In: Advances in Cryptology EUROCRYPT. Berlin: Springer, 2005. 457–473
58 Goyal V, Pandey O, Sahai A, et al. Attribute-based encryption for fine-grained access control of encrypted data. In: Proceedings of the 13th ACM Conference on Computer and Communications Security. New York: ACM, 2006. 89–98
59 Bethencourt J, Sahai A, Waters B. Ciphertext-policy attribute-based encryption. In: Proceedings of the 2007 IEEE Symposium on Security and Privacy Computer Society, Berkeley, 2007. 321–334
60 Chen J, Gay R, Wee H. Improved dual system ABE in prime-order groups via predicate encodings. In: Advances in Cryptology EUROCRYPT. Berlin: Springer, 2015. 595–624
61 Garg S, Gentry C, Sahai A, et al. Witness encryption and its applications. In: Proceedings of the 45th Annual ACM Symposium on Theory of Computing. New York: ACM, 2013. 467–476
62 Gentry C, Lewko A B, Waters B. Witness encryption from instance independent assumptions. In: Advances in Cryptology CRYPTO. Berlin: Springer, 2014. 426–443
63 Waters B. Functional encryption: origins and recent developments. In: Public-Key Cryptography PKC. Berlin: Springer, 2013. 51–54
64 Barbosa M, Farshim P. On the semantic security of functional encryption schemes. In: Public-Key Cryptography PKC. Berlin: Springer, 2013. 143–161
65 Farràs O, Hansen T, Kaced T, et al. Optimal non-perfect uniform secret sharing schemes. In: Advances in Cryptology CRYPTO. Berlin: Springer, 2014. 217–234
66 Boyle E, Gilboa N, Ishai Y. Function secret sharing. In: Advances in Cryptology EUROCRYPT. Berlin: Springer, 2015. 337–367
67 Jarecki S, Kiayias A, Krawczyk H. Round-optimal password-protected secret sharing and t-pake in the password-only model. In: Advances in Cryptology ASIACRYPT. Berlin: Springer, 2014. 233–253
68 Cramer R, Damgård I B, Döttling N, et al. Linear secret sharing schemes from error correcting codes and universal hash functions. In: Advances in Cryptology EUROCRYPT. Berlin: Springer, 2015. 313–336
69 Goldwasser S, Micali S, Rackoff C. The knowledge complexity of interactive proof-systems. In: Proceedings of the 17th Annual ACM Symposium on Theory of Computing. New York: ACM, 1985. 291–304
70 De Santis A, Micali S, Persiano G. Non-interactive zero-knowledge proof systems. In: Advances in Cryptology CRYPTO. Berlin: Springer, 1988. 52–72
71 BFM M B, Feldman P, Micali S. Non-interactive zero-knowledge proof systems and applications. In: Proceedings of the 20th Annual Symposium on Theory of Computing. New York: ACM, 1988. 103–112
72 Deng Y, Lin D D. Instance-dependent verifiable random functions and their application to simultaneous resettability. In: Advances in Cryptology EUROCRYPT. Berlin: Springer, 2007. 148–168
73 Deng Y, Goyal V, Sahai A. Resolving the simultaneous resettability conjecture and a new non-black-box simulation strategy. In: 50th Annual IEEE Symposium on Foundations of Computer Science (FOCS'09), Atlanta, 2009. 251–260
74 Yao C C, Yung M, Zhao Y L. Concurrent Knowledge Extraction in Public-Key Models. J Cryptology, in press, doi: 10.1007/s00145-014-9191-z
75 Goyal V, Jain A, Ostrovsky R, et al. Constant-round concurrent zero knowledge in the bounded player model. In: Advances in Cryptology ASIACRYPT. Berlin: Springer, 2013. 21–40
76 Unruh D. Non-interactive zero-knowledge proofs in the quantum random oracle model. In: Advances in Cryptology EUROCRYPT. Berlin: Springer, 2015. 755–784
77 Kiltz E, Wee H. Quasi-adaptive nizk for linear subspaces revisited. In: Advances in Cryptology EUROCRYPT. Berlin: Springer, 2015. 101–128
78 Yao A. Protocols for secure computations. FOCS. 1982, 82: 160–164
79 Goldreich O, Micali S, Wigderson A. How to play any mental game. In: Proceedings of the 19th Annual ACM Symposium on Theory of Computing. New York: ACM, 1987. 218–229
80 Garay J, Kiayias A, Leonardos N. The bitcoin backbone protocol: analysis and applications. In: Advances in Cryptology EUROCRYPT. Berlin: Springer, 2015. 281–310
81 Asharov G, Lindell Y, Schneider T, et al. More efficient oblivious transfer extensions with security for malicious adversaries. In: Advances in Cryptology EUROCRYPT. Berlin: Springer, 2015. 673–701
82 Goldwasser S. Multi party computations: past and present. In: Proceedings of the 16th Annual ACM Symposium on Principles of Distributed Computing. New York: ACM, 1997. 1–6
83 Kiyoshima S. Round-efficient black-box construction of composable multi-party computation. In: Advances in Cryptology-CRYPTO. Berlin: Springer, 2014. 351–368

84 Ishai Y, Ostrovsky R, Zikas V. Secure multi-party computation with identifiable abort. In: Advances in Cryptology CRYPTO. Berlin: Springer, 2014. 369–386
85 Beimel A, Gabizon A, Ishai Y, et al. Non-interactive secure multiparty computation. In: Advances in Cryptology CRYPTO. Berlin: Springer, 2014. 387–404
86 Wang C, Ren K, Wang J. Secure and practical outsourcing of linear programming in cloud computing. In: Proceedings of IEEE INFOCOM'11, Shanghai, 2011. 820–828
87 Gentry C, Halevi S, Raykova M, et al. Outsourcing private ram computation. In: IEEE 55th Annual Symposium on Foundations of Computer Science (FOCS), Philadelphia, 2014. 404–413
88 Sheng B, Li Q. Verifiable privacy-preserving sensor network storage for range query. IEEE Trans Mobile Comput, 2011, 10: 1312–1326
89 Cui H, Mu Y, Au M H. Proof of retrievability with public verifiability resilient against related-key attacks. IET Inform Secur, 2014, 9: 43–49
90 Kocher P C. Timing attacks on implementations of diffie-hellman, RSA, DSS, and other systems. In: Advances in Cryptology CRYPTO. Berlin: Springer, 1996. 104–113
91 Kelsey J, Schneier B, Wagner D, et al. Side channel cryptanalysis of product ciphers. In: Computer Security ESORICS. Berlin: Springer, 1998. 97–110
92 Dhem J F, Koeune F, Leroux P A, et al. A practical implementation of the timing attack. In: Smart Card Research and Applications. Berlin: Springer, 2000. 167–182
93 Boneh D, DeMillo R A, Lipton R J. On the importance of checking cryptographic protocols for faults. In: Advances in Cryptology EUROCRYPT. Berlin: Springer, 1997. 37–51
94 Joye M, Lenstra A K, Quisquater J J. Chinese remaindering based cryptosystems in the presence of faults. J Cryptol, 1999, 12: 241–245
95 Kocher P, Jaffe J, Jun B. Differential power analysis. In: Advances in Cryptology CRYPTO. Berlin: Springer, 1999. 388–397
96 Quisquater J J, Samyde D. A new tool for non-intrusive analysis of smart cards based on electromagnetic emissions. In: Eurocrypt 2000 Rump Session, Bruges (Brugge), 2000
97 Gandolfi K, Mourtel C, Olivier F. Electromagnetic analysis: concrete results. In: Cryptographic Hardware and Embedded Systems-CHES. Berlin: Springer, 2001. 251–261
98 Belaid S, Fouque P A, Gérard B. Side-Channel Analysis of Multiplications in $GF(2^{128})$. In: Advances in Cryptology ASIACRYPT. Berlin: Springer, 2014. 306–325
99 Lomné V, Prouff E, Roche T. Behind the scene of side channel attacks. In: Advances in Cryptology ASIACRYPT. Berlin: Springer, 2013. 506–525
100 Petit C, Standaert F X, Pereira O, et al. A block cipher based pseudo random number generator secure against side-channel key recovery. In: Proceedings of the ACM Symposium on Information Computer and Communications Security. New York: ACM, 2008. 56–65
101 Dziembowski S, Pietrzak K. Leakage-resilient cryptography. In: Proceedings of the 49th Annual IEEE Symposium on Foundations of Computer Science (FOCS'08), Philadelphia, 2008. 293–302
102 Dachman-Soled D, Liu F H, Zhou H S. Leakage-resilient circuits revisited-optimal number of computing components without leak-free hardware. In: Advances in Cryptology EUROCRYPT. Berlin: Springer, 2015. 131–158
103 Dziembowski S, Faust S, Skorski M. Noisy leakage revisited. In: Advances in Cryptology EUROCRYPT. Berlin: Springer, 2015. 159–188
104 Longo J, Martin D P, Oswald E, et al. Simulatable leakage: analysis, pitfalls, and new constructions. In: Advances in Cryptology ASIACRYPT. Berlin: Springer, 2014. 223–242
105 Bitansky N, Dachman-Soled D, Lin H. Leakage-tolerant computation with input-independent preprocessing. In: Advances in Cryptology CRYPTO. Berlin: Springer, 2014. 146–163
106 Yu Y, Standaert F X, Pereira O, et al. Practical leakage-resilient pseudorandom generators. In: Proceedings of the 17th ACM Conference on Computer and Communications Security. New York: ACM, 2010. 141–151
107 Standaert F X, Pereira O, Yu Y. Leakage-resilient symmetric cryptography under empirically verifiable assumptions. In: Advances in Cryptology CRYPTO. Berlin: Springer, 2013. 335–352
108 Chow S, Eisen P A, Johnson H, et al. White-box cryptography and an AES implementation. In: Selected Areas in Cryptography. Berlin: Springer, 2003. 250–270
109 Xiao Y, Lai X. A secure implementation of white-box AES. In: Proceedings of the 2nd International Conference on Computer Science and its Applications (CSA'09), 2009. 1–6
110 Mulder Y D, Roelse P, Preneel B. Cryptanalysis of the Xiao-Lai white-box AES implementation. In: Selected Areas in Cryptography. Berlin: Springer, 2013. 34–49
111 Garg S, Gentry C, Halevi S, et al. Candidate indistinguishability obfuscation and functional encryption for all circuits. In: Proceedings of the IEEE 54th Annual Symposium on Foundations of Computer Science (FOCS), Berkeley, 2013. 40–49
112 Cherkaoui A, Fischer V, Fesquet L, et al. A very high speed true random number generator with entropy assessment.

In: Cryptographic Hardware and Embedded Systems-CHES. Berlin: Springer, 2013. 179–196
113 Fischer V, Lubicz D. Embedded evaluation of randomness in oscillator based elementary TRNG. In: Cryptographic Hardware and Embedded Systems-CHES. Berlin: Springer, 2014. 527–543
114 Ma Y, Lin J, Chen T, et al. Entropy evaluation for oscillator-based true random number generators. In: Cryptographic Hardware and Embedded Systems-CHES. Berlin: Springer, 2014. 544–561
115 Ravikanth P, Ben R, Jason T, et al. Physical one-way function. Science, 2002, 297: 2026–2030
116 Delvaux J, Gu D, Schellekens D, et al. Secure lightweight entity authentication with strong pufs: mission impossible. In: Cryptographic Hardware and Embedded Systems-CHES. Berlin: Springer, 2014. 451–475
117 Lu M X, Lai X J, Xiao G Z, et al. A symmetric-key cryptosystem with DNA technology. Sci China Ser F-Inf Sci, 2007, 50: 324–333
118 Lai X J, Lu M X, Qin L, et al. Asymmetric encryption and signature method with DNA technology. Sci China Inf Sci, 2010, 53: 506–514
119 Bennett C H, Brassard G. Quantum cryptography: public key distribution and coin tossing. In: International Conference on Computer System and Signal Processing, Bangalore, 1984. 175–179
120 Bennett C H. Quantum cryptography using any two nonorthogonal states. Phys Rev Lett, 1992, 68: 3121–3124
121 Barak B, Goldreich O, Impagliazzo R, et al. On the (im)possibility of obfuscating programs. J ACM, 2012, 59: 1–48
122 Brakerski Z, Gentry C, Vaikuntanathan V. (Leveled) Fully homomorphic encryption without bootstrapping. In: Proceedings of the 3rd Innovations in Theoretical Computer Science Conference. New York: ACM, 2012. 309–325
123 Böhl F, Hofheinz D, Jager T, et al. Practical signatures from standard assumptions. In: Advances in Cryptology EUROCRYPT. Berlin: Springer, 2013. 461–485
124 Brakerski Z, Vaikuntanathan V. Efficient fully homomorphic encryption from (standard) LWE. SIAM J Comput, 2014, 43: 831–871
125 Cash D, Hofheinz D, Kiltz E, et al. Bonsai trees, or how to delegate a lattice basis. J Cryptol, 2012, 25: 601–639
126 Lo H K, Curty M, Qi B. Measurement-device-independent quantum key distribution. Phys Rev Lett, 2012, 108: 130503
127 Pawlowski M, Brunner N. Semi-device-independent security of one-way quantum key distribution. Phys Rev A, 2011, 84: 010302
128 Vazirani U, Vidick T. Fully device-independent quantum key distribution. Phys Rev Lett, 2014, 113: 140501
129 Gentry C. Fully homomorphic encryption using ideal lattices. In: Proceedings of the 41st Annual ACM Symposium on Theory of Computing. New York: ACM Press, 2009, 9: 169–178
130 Brakerski Z, Vaikuntanathan V. Efficient fully homomorphic encryption from (standard) LWE. SIAM J Comput, 2014, 43: 831–871
131 Regev O. On lattices, learning with errors, random linear codes, and cryptography. J ACM, 2005, 56: 84–93
132 Peikert C. Public-key cryptosystems from the worst-case shortest vector problem. In: Proceedings of the 41 Annual ACM Symposium on Theory of Computing. New York: ACM, 2009. 333–342
133 Gentry C, Peikert C, Vaikuntanathan V. Trapdoors for hard lattices and new cryptographic constructions. In: Proceedings of the 40th Annual ACM Symposium on Theory of Computing. New York: ACM, 2008. 197–206
134 Cash D, Hofheinz D, Kiltz E, et al. Bonsai trees, or how to delegate a lattice basis. J Cryptol, 2012, 25: 601–639
135 Ducas L, Lyubashevsky V, Prest T. Efficient identity-based encryption over NTRU lattices. In: Advances in Cryptology ASIACRYPT. Berlin: Springer, 2014. 22–41
136 Lyubashevsky V. Lattice signatures without trapdoors. In: Advances in Cryptology EUROCRYPT. Berlin: Springer, 2012. 738–755
137 Micciancio D, Peikert C. Trapdoors for lattices: Simpler, tighter, faster, smaller. In: Advances in Cryptology EUROCRYPT. Berlin: Springer, 2012. 700–718
138 Ducas L, Durmus A, Lepoint T, et al. Lattice signatures and bimodal Gaussians. In: Advances in Cryptology CRYPTO. Berlin: Springer, 2013. 40–56
139 Böhl F, Hofheinz D, Jager T, et al. Practical signatures from standard assumptions. In: Advances in Cryptology EUROCRYPT. Berlin: Springer, 2013. 461–485
140 Zhang J, Zhang Z, Ding J, et al. Authenticated key exchange from ideal lattices. In: Advances in Cryptology EUROCRYPT. Berlin: Springer, 2015. 719–751
141 Peikert C, Vaikuntanathan V, Waters B. A framework for efficient and composable oblivious transfer. In: Advances in Cryptology CRYPTO. Berlin: Springer, 2008. 554–571
142 Lyubashevsky V, Micciancio D, Peikert C, et al. SWIFFT: a modest proposal for FFT hashing. In: Fast Software Encryption. Berlin: Springer, 2008. 54–72
143 Lyubashevsky V, Peikert C, Regev O. On ideal lattices and learning with errors over rings. J ACM, 2013, 60: 1–23
144 Gentry C. Fully homomorphic encryption using ideal lattices. In: Proceedings of the 41 Annual ACM Symposium on Theory of Computing. New York: ACM, 2009. 169–178
145 Brakerski Z, Gentry C, Vaikuntanathan V. (Leveled) Fully homomorphic encryption without bootstrapping. ACM Trans Comput Theory, 2014, 6: 169–178

146 Alperin-Sheriff J, Peikert C. Practical bootstrapping in quasilinear time. In: Advances in Cryptology CRYPTO. Berlin: Springer, 2013. 1–20
147 Alperin-Sheriff J, Peikert C. Faster bootstrapping with polynomial error. In: Advances in Cryptology CRYPTO. Berlin: Springer, 2014. 297–314
148 Rohloff K, Cousins D B. A scalable implementation of fully homomorphic encryption built on NTRU. In: Financial Cryptography and Data Security. Berlin: Springer, 2014. 221–234
149 Rohloff K. Enabling practical, secure computing through fully homomorphic encryption. DIMACS Workshop on Multicore and Cryptography, Stevens Institute of Technology, Hoboken, 2014, 22
150 Sahai A, Waters B. How to use indistinguishability obfuscation: deniable encryption, and more. In: Proceedings of the 46th Annual ACM Symposium on Theory of Computing. New York: ACM, 2014. 475–484
151 Hohenberger S, Sahai A, Waters B. Replacing a random oracle: full domain hash from indistinguishability obfuscation. In: Advances in Cryptology EUROCRYPT. Berlin: Springer, 2014. 201–220
152 Gentry C, Lewko A B, Sahai A, et al. Indistinguishability obfuscation from the multilinear subgroup elimination assumption. IACR Cryptol ePrint Archive, 2014, 2014: 309
153 Ananth P, Gupta D, Ishai Y, et al. Optimizing obfuscation: avoiding barrington's theorem. In: Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security. New York: ACM, 2014. 646–658
154 Cheon J H, Han K, Lee C, et al. Cryptanalysis of the multilinear map over the integers. In: Advances in Cryptology EUROCRYPT. Berlin: Springer, 2015. 3–12
155 Hu Y P, Jia H W. Cryptanalysis of GGH Map. Cryptology ePrint Archive, Report 2015/301, 2015
156 Millan W, Clark A, Dawson E. Smart hill climbing finds better Boolean functions. In: International Conference on Information and Communication Security, Beijing, 1997. 50–63
157 Clark J A, Jacob J L. Two-stage optimisation in the design of Boolean functions. In: Information Security and Privacy. Berlin: Springer, 2000. 242–254
158 Zhang H G, Feng X T, Qin Z P, et al. Evolutionary cryptosystems and evolutionary design for DES. J China Inst Commun, 2002, 23: 57–64 [张焕国, 冯秀涛, 覃中平, 等. 演化密码与 DES 密码的演化设计. 通信学报, 2002, 23: 57–64]
159 Zhang H G, Feng X T, Qin Z P, et al. Evolutionary cryptosystems and evolutionary design for DES. Chinese J Comput, 2003, 26: 1678–1684 [张焕国, 冯秀涛, 覃中平, 等. 演化密码与 DES 的演化研究. 计算机学报, 2003, 26: 1678–1684]
160 ITU-T. Future networks: objectives and design goals. Y.3001. http://www.itu.int/rec/T-REC-Y.3001-201105-I. 2011
161 Lai B, Kim S, Verbauwhede I. Scalable session key construction protocol for wireless sensor networks. In: IEEE Workshop on Large Scale RealTime and Embedded Systems (LARTES), Austin, 2002. 7
162 Alliance Z B. Zigbee Specification Document 053474r06, v1.0. Technical report, ZigBee Alliance, 2004.ITU-T, Y.300
163 Dutertre B, Cheung S, Levy J. Lightweight Key Management in Wireless Sensor Networks by Leveraging Initial Trust. Technical Report SRI-SDL-04-02, SRI International, 2004
164 Chan H, Gligor V D, Perrig A, et al. On the distribution and revocation of cryptographic keys in sensor networks. IEEE Trans Dependable Secure Comput, 2005, 2: 233–247
165 Gupta A, Kuri J. Deterministic schemes for key distribution in wireless sensor networks. In: Proceedings of the 3rd International Conference on Communication Systems Software and Middlewareand Workshops (COMSWARE'08), IEEE Computer Society, Washington, 2008. 452–459
166 Hwang D D, Lai B C C, Verbauwhede I. Energy-memory-security tradeoffs in distributed sensor networks. In: ADHOC, Mobile, and Wireless Networks. Berlin: Springer, 2004. 70–81
167 Shan T H, Liu C M. Enhancing the key pre-distribution scheme on wireless sensor networks. In: Asia-Pacific Services Computing Conference, APSCC'08 IEEE, Yilan, 2008. 1127–1131
168 Chan H, Perrig A, Song D. Random key predistribution schemes for sensor networks. In: Proceedings of the IEEE Symposium on Security and Privacy (SP'03), IEEE Computer Society, Washington, 2003. 197–213
169 Law C F, Hung K S, Kwok Y K. A novel key redistribution scheme for wireless sensor networks. In: IEEE International Conference on Communications (ICC'07), IEEE Computer Society, Washington, 2007. 3437–3442
170 IEEE. IEEE standard for local and metropolitan area networks: port-based network access control. IEEE 820.1X-2010. http://standards.ieee.org/findstds/standard/802.1X-2010.html. 2010
171 IEEE. Wireless medium access control (MAC) and physical layer (PHY) specifications: medium acess control (MAC) security. IEEE STD 802.11i/D4. http://standards.ieee.org/findstds/interps/802.11i-2004.html. 2004
172 Allen J, Wilson J. Securing a wireless network. In: Proceedings of the 30th Annual ACM SIGUCCS Conference on User Services. New York: ACM, 2002. 213–215
173 Li X, Bao F, Li S, et al. FLAP: an efficient WLAN initial access authentication protocol. IEEE Trans Parallel Distrib Syst, 2014, 25: 488–497
174 Zhu J, Ma J. A new authentication scheme with anonymity for wireless environments. IEEE Trans Consum Electron, 2004, 50: 231–235
175 Jiang Q, Ma J, Li G, et al. An enhanced authentication scheme with privacy preservation for roaming service in

global mobility networks. Wirel Personal Commun, 2013, 68: 1477–1491
176 Doraswamy N, Harkins D. IPSec: the new security standard for the internet, intranets, and virtual private networks. Upper Saddle River: Prentice Hall Professional, 2003
177 Rescorla E. SSL and TLS: designing and building secure systems. Indianapolis: Addison-Wesley, 2001
178 Patil A, Sawant H K. Technical specification group services and system aspects, IP multimedia subsystem (IMS). IJECCE, 2012, 3: 234–238
179 Idrissi Y, Zahid N, Jedra M. Security analysis of 3GPP (LTE)-WLAN interworking and a new local authentication method based on EAP-AKA. In: International Conference on Future Generation Communication Technology (FGCT), London, 2012. 137–142
180 Jiang Q, Ma J F, Li G S, et al. The amalgamation based on WAPI end WLAN. Chinese J Comput, 2010, 33: 1675–1686 [姜奇, 马建峰, 李光松, 等. 基于 WAPI 的 WLAN 与 3G 网络安全融合. 计算机学报, 2010, 33: 1675–1686]
181 Yao C C, Zhao Y. OAKE: a new family of implicitly authenticated diffie-hellman protocols. In: Proceedings of the 2013 ACM SIGSAC Conference on Computer and Communications Security. New York: ACM, 2013. 1113–1128
182 Raymond D R, Marchany R C, Brownfield M, et al. Effects of Denial-of-Sleep Attacks on Wireless Sensor Network MAC Protocols. IEEE Trans Veh Tech, 2009, 58: 367–380
183 Wood A D, Stankovic J A. Denial of service in sensor networks. IEEE Comput, 2002, 10: 54–62
184 Hu Y C, Perrig A, Johnson D B. Wormhole Detection in Wireless Ad Hoc Networks. Technical Report TR01384. 2002
185 Perrig A, Stankovic J, Wagner D. Security in wireless sensor networks. Commun ACM, 2004, 47: 53–57
186 NEEDHAM A B Y R, Lampson B. Network Attack and Defense. White Paper, 2008
187 Trostle J, Van Besien B, Pujari A. Protecting against DNS cache poisoning attacks. In: Proceedings of 6th IEEE Workshop on Secure Network Protocols (NPSec), Kyoto, 2010. 25–30
188 La Polla M, Martinelli F, Sgandurra D. A survey on security for mobile devices. Commun Surv Tutorials, 2013, 15: 446–471
189 Idika N, Mathur A P. A Survey of Malware Detection Techniques. Technical Report, Purdue University, 2007, 48
190 Ferraiolo D F, Sandhu R, Gavrila S, et al. Proposed NIST standard for role-based access control. ACM Trans Inf Syst Secur (TISSEC), 2001, 4: 24–274
191 Thomas R K, Sandhu R S. Task-based authorization controls (TBAC): a family of models for active and enterprise-oriented authorization management. In: Proceedings of the Ifip Wg11 Workshop on Database Security, California, 1999. 166–181
192 Goyal V, Pandey O, Sahai A, et al. Attribute-based encryption for fine-grained access control of encrypted data. In: Proceedings of the 13th ACM Conference on Computer and Communications Security. New York: ACM, 2006. 89–98
193 Yang K, Jia X, Ren K, et al. Enabling efficient access control with dynamic policy updating for big data in the cloud. In: Proceedings of IEEE INFOCOM, Toronto, 2014. 2013–2021
194 Jose J, Jose J, Princy M. A survey on privacy preserving data aggregation protocols for wireless sensor networks. J Comput Inf Tech, 2014, 22: 1–20
195 Sweeney L. K-anonymity: a model for protecting privacy. Int J Uncertainty, Fuzz Knowledge-Based Syst, 2002, 10: 557–570
196 Machanavajjhala A, Kifer D, Gehrke J, et al. L-diversity: privacy beyond k-anonymity. ACM Trans Knowl Discov Data (TKDD), 2007, 1: 1–52
197 Dwork C. Differential privacy. In: Encyclopedia of Cryptography and Security. Berlin: Springer, 2011. 338–340
198 Jose J, Jose J, Princy M. A survey on privacy preserving data aggregation protocols for wireless sensor networks. J Comput Inf Tech, 2014, 22: 1–20
199 Xi N, Sun C, Ma J, et al. Secure service composition with information flow control in service clouds. Future Gener Comput Syst, 2015, 49: 142–148
200 Makhlouf A, Boudriga N. Intrusion and anomaly detection in wireless networks. In: Zhang Y, Zheng J, Ma M, eds. Handbook of Research on Wireless Security. Hershey: Information Science Publishing, 2008
201 Haataja K. Security Threats and Countermeasures in Bluetooth-enabled Systems. Kuopio: University of Kuopio, 2009
202 Xie L, Zhang X, Seifert J P, et al. pBMDS: a behavior-based malware detection system for cellphone devices. In: Proceedings of the 3rd ACM Conference on Wireless Network Security. New York: ACM, 2010. 37–48
203 Becher M, Freiling F C. Towards dynamic malware analysis to increase mobile device security. In: Proceedings of SICHERHEIT, 2008. 423–433
204 Traynor P, Lin M, Ongtang M, et al. On cellular botnets: measuring the impact of malicious devices on a cellular network core. In: Proceedings of the 16th ACM Conference on Computer and Communications Security. New York: ACM, 2009. 223–234
205 Enck W, Traynor P, McDaniel P, et al. Exploiting open functionality in SMS-capable cellular networks. In: Proceedings of the 12th ACM Conference on Computer and Communications Security. New York: ACM, 2005. 393–404

206 Michael B, Felix C F, Johannes H, et al. Mobile security catching upon revealing the nuts and bolts of the security of mobile devices. In: IEEE Symposium on Security and Privacy, Berkeley, 2011. 96–111
207 Becher M. Security of smartphones at the dawn of their ubiquitousness. Dissertation Ph.D. Degree. Mannheim: University of Mannheim, 2009
208 Hepner C, Zmijewski E. Defending against BGP man-in-the-middle attacks. In: Black Hat DC Conference, Arlington, 2009
209 Waichal S, Meshram B B. Router attacks-detection and defense mechanisms. Int J Sci Technol Res, 2013, 2: 145–149
210 Weaver N, Sommer R, Paxson V. Detecting forged TCP reset packets. In: Proceedings of 16th Network and Distributed Security Symposium (NDSS), San Diego, 2009
211 Nakibly G, Kirshon A, Gonikman D, et al. Persistent OSPF attacks. In: Proceedings of 19th Network and Distributed Security Symposium (NDSS), San Diego, 2012
212 Jones E, Moigne O L. OSPF security vulnerabilities analysis. http://tools.ietf.org/html/draft-ietf-rpsec-ospf-vuln-02. 2006
213 Shaikh A, Greenberg A. Experience in black-box OSPF measurement. In: Proceedings of the 1st ACM SIGCOMM Workshop on Internet Measurement. New York: ACM, 2001. 113–125
214 Hartman S, Wasserman M, Zhang D. Security requirements in the software defined networking model. IETF Draft (draft-hartman-sdnsec-requirements), http://tools.ietf.org/html/draft-hartman-sdnsec-requirements-00. 2013
215 Hardt D. The OAuth 2.0 authorization framework. http://tools.ietf.org/html/rfc6749.html. 2012
216 Porras P, Shin S, Yegneswaran V, et al. A security enforcement kernel for OpenFlow networks. In: Proceedings of the 1st Workshop on Hot Topics in Software Defined Networks. New York: ACM, 2012. 121–126
217 Shin S, Porras P A, Yegneswaran V, et al. FRESCO: modular composable security services for software-defined networks. In: Proceedings of 20th Network and Distributed Security Symposium (NDSS), San Diego, 2013
218 Anand M, Cronin E, Sherr M, et al. Security challenges in next generation cyber physical systems. In: Beyond SCADA: Network Embedded Control Cyber Physical Systems, Pittsburgh, 2006
219 Shafi Q. Cyber physical systems security: a brief survey. In: 12th International Conference on Computational Science and Its Applications, Salvador, 2012. 146–150
220 Fletcher K K, Liu X F. Security requirements analysis, specification, prioritization and policy development in cyber-physical systems. In: 5th International Conference on Secure Software Integration and Reliability Improvement Companion (SSIRI-C), Jeju Island, 2011. 106–113
221 Azab M, Eltoweissy M. Defense as a service cloud for cyber-physical systems. In: 7th International Conference on Collaborative Computing: Networking, Applications and Worksharing (CollaborateCom), Orlando, 2011. 392–401
222 Lee G S, Thuraisingham B. Cyberphysical systems security applied to telesurgical robotics. Comput Stand Inter, 2012, 34: 225–229
223 Gohil A, Modi H, Patel S K. 5G technology of mobile communication: a survey. In: International Conference on Intelligent Systems and Signal Processing (ISSP), Gujarat, 2013. 288–292
224 Chin W H, Fan Z, Haines R. Emerging technologies and research challenges for 5G wireless networks. Wirel Commun, 2014, 21: 106–112
225 沈昌祥, 张焕国, 王怀民, 等. 可信计算的研究与发展, 中国科学: 信息科学, 2010, 40: 139–380
226 Shen C X, Zhang H G, Wang H M, et al. Research on trusted computing and its development. Sci China Inf Sci, 2010, 53: 405–433
227 张焕国, 严飞, 傅建明, 等. 可信计算平台测评理论与关键技术研究. 中国科学: 信息科学, 2010, 40: 167–188
228 Zhang H G, Yan F, Fu J M, et al. Research on theory and key technology of trusted computing platform security testing and evaluation. Sci China Inf Sci, 2010, 53: 434–453
229 Zhang H G, Wu G Q, Qin Z P, et al. A new type secure computer. J Wuhan Univ (SCIENCE EDITION), 2004, 50: 1–6 [张焕国, 毋国庆, 覃中平, 等. 一种新型安全计算机. 武汉大学学报 (理学版), 2004, 50: 1–6]
230 Zhang H G, Liu Y Z, Yu F J, et al. A new embedded security module. J Wuhan Univ (SCIENCE EDITION), 2004, 50: 7–11 [张焕国, 刘玉珍, 余发江, 等. 一种新型嵌入式安全模块. 武汉大学学报 (理学版), 2004, 50: 7–11]
231 Trusted Platform Module Specifications. http://www.trustedcomputinggroup.org/developers/trusted_platform_module. 2015
232 Zhang Q Y, Zhao S J, Qin Y, et al. Formal analysis of TPM 2.0 key management APIs. Chinese Sci Bull, 2014, 59: 4210-4224
233 Chen L, Li J. Flexible and scalable digital signatures in TPM 2.0. In: Proceedings of the 2013 ACM SIGSAC Conference on Computer and Communications Security. New York: ACM, 2013. 37–48
234 Xu Y, Zhao B. TPM 2.0 key replication security enhancement scheme. J Wuhan Univ (SCIENCE EDITION), 2014, 60: 471–477 [徐阳, 赵波, 等. TPM 2.0 密钥复制安全性增强方案. 武汉大学学报 (理学版), 2014, 60: 471–477]
235 Wu K, Zhao B, Milan-Heinayati, et al. Security defects of TPM 2.0 policy authorization mechanism and its improvement scheme. J Wuhan Univ (Sci ed), 2014, 60: 478–484 [吴凯, 赵波, 米兰 - 黑娜亚提, 等. TPM 2.0 策略授权机制的安全缺陷及其改进方案. 武汉大学学报 (理学版), 2014, 60: 478–484]
236 Yu F J, Zhang H G, Zhao B, et al. A formal analysis of Trusted Platform Module 2.0 HMAC authorization under

DRM scenario. Secur Commun Netw, in press, doi: 10.1002/sec.1193
237 Liu Z W, Feng D G. Dynamic integrity measurement framework based on trusted computing. Electron Inf Tech, 2010, 32: 875–879 [刘孜文, 冯登国. 基于可信计算的动态完整性度量架构. 电子与信息学报, 2010, 32: 875–879]
238 Yan F, Shi X, Li Z H, et al. A design and implementation of UEFI based virtual machine dynamic security measurement framework. J Sichuan Univ (Engineering Science Edition), 2014, 1: 22–28 [严飞, 石翔, 李志华, 等. 一种基于UEFI 的虚拟机动态安全度量框架设计与实现. 四川大学学报 (工程科学版), 2014, 1: 22–28]
239 Hu H S. A design and implementation of IaaS dynamic measurement protocol. Dissertation for Master's Degree. Wuhan: Wuhan University, 2015 [胡海生. 一种 IaaS 动态度量协议的设计与实现. 硕士学位论文. 武汉: 武汉大学, 2015]
240 Wang L N, Yu R W, Gao H J, et al. Trusted virtual machine execution environment construction method based on trust extension. J Commun, 2011, 32: 1–8 [王丽娜, 高汉军, 余荣威, 等. 基于信任扩展的可信虚拟机执行环境构建方法研究. 通信学报, 2011, 32: 1–8]
241 Yang S L. Virtual trusted platform and its security research based on TPM 2.0. Dissertation for Master's Degree. Wuhan: Wuhan University, 2015 [杨妹黎. 基于 TPM 2.0 的虚拟可信平台及其安全性研究. 硕士学位论文. 武汉: 武汉大学, 2015]
242 Dai W, Jin H, Zou D, et al. TEE: a virtual DRTM based execution environment for secure cloud-end computing. In: Proceedings of the 17th ACM Conference on Computer and Communications Security. New York: ACM, 2010. 663–665
243 Zou D Q, Zhang W R, Qiang W Z, et al, Design and implementation of a trusted monitoring framework for cloud platform. Future Generation Comput Syst, 2013, 29: 2092–2102
244 Zhang H G, Mao S W, Wang Ho Z. Asymmetric-computing Type Shared Key Establishing Method Suitable for Cloud Computing and IoT. Patent: US14/724809
245 Mei H, Wang Q X, Zhang L, et al. Progress on software analysis techniques. J Softw, 2009, 32: 1697–1701 [梅宏, 王千祥, 张路, 等. 软件分析技术进展. 软件学报, 2009, 32: 1697–1701]
246 Fang B X, Lu T B, Li C. Progress on software assurance. J Commun, 2009, 30: 106–122 [方滨兴, 陆天波, 李超. 软件确保研究进展. 通信学报, 2009, 30: 106–122]
247 Marquardt P, Verma A, Carter H, et al. (sp) iPhone: decoding vibrations from nearby keyboards using mobile phone accelerometers. In: Proceedings of the 18th ACM Conference on Computer and Communications Security. New York: ACM, 2011. 551–562
248 Lin C C, Li H, Zhou X, et al. Screenmilker: how to milk your android screen for secrets. In: Proceedings of 21st Annual Network and Distributed System Security Symposium (NDSS), San Diego, 2014. 1–14
249 Michalevsky Y, Nakibly G, Schulman A, et al. PowerSpy: location tracking using mobile device power analysis. arXiv: 1502.03182, 2015
250 Fu J M, Du H, Peng B C. Dynamic detection of a component loading vulnerability. J Tsinghua Univ (NATURAL SCIENCE EDITION), 2012, 52: 1356–1363 [傅建明, 杜浩, 彭碧琛. 一种组件加载漏洞的动态检测. 清华大学学报(自然科学版), 2012, 52: 1356–1363]
251 Hsu F H, Tso C K, Yeh Y C, et al. BrowserGuard: a behavior-based solution to drive-by-download attacks. IEEE J Sel Areas Commun, 2011, 29: 1461–1468
252 Forrest S, Somayaji A, Ackley D H. Building diverse computer systems. In: the 6th Workshop on Hot Topics in Operating Systems, Cape Cod, 1997. 67–72
253 Lu L, Yegneswaran V, Porras P, et al. Blade: an attack-agnostic approach for preventing drive-by malware infections. In: Proceedings of the 17th ACM conference on Computer and communications security (CCS'2010). New York: ACM, 2010. 440–450
254 Song C, Zhuge J, Han X, et al. Preventing drive-by download via inter-module communication monitoring. In: Proceedings of the 5th ACM Symposium on Information, Computer and Communications Security. New York: ACM, 2010. 124–134
255 ARM Security Technology—Building a Secure System using TrustZone Technology. ARM Technical White Paper, 2005–2009
256 Rosenberg D. Qsee trustzone kernel integer over flow vulnerability. In: Black Hat Conference, Las Vega, 2014
257 Jeffrey M, Park S, Lee K, et al. Content security for IPTV. IEEE Commun Mag, 2008, 46: 138–146
258 Meike M, Sametinger J, Wiesauer A. Security in open source web content management systems. IEEE Secur Priv, 2009, 7: 44–51
259 Li Q, Lui J C S, Chiu D M. On the security and efficiency of content distribution via network coding. IEEE Trans Depend Secure Comput, 2012, 9: 211–221
260 Chen X X, Fang B X, HU M, et al. A new field in security of internet information and content—network information penetration detection technology. J China Inst Commun, 2004, 25: 185–191 [陈训逊, 方滨兴, 胡铭, 等. 一个网络信息内容安全的新领域 —— 网络信息渗透检测技术. 通信学报, 2004, 25: 185–191]
261 Ge L, Ji X S, Jiang T. Research on situation awareness model of information content security incidents in telecommunication network. Telecommun Sci, 2014, 2: 14–20 [葛琳, 季新生, 江涛. 电信网信息内容安全事件态势感知模

型研究. 电信科学, 2014, 2: 14–20]
262 Balabanovic M, Shoham Y. Learning information retrieval agents: experiments with automated web browsing. Online Working Notes of the AAAI Spring Symposium Series on Information Gathering from Distributed, Heterogeneous Environments, 1995. 13–18
263 Teufel B, Schmidt S. Full text retrieval based on syntactic similarities. Inform Syst, 1988, 13: 65–70
264 Letsche T A, Berry M W. Large-scale information retrieval with latent semantic indexing. Inform Sci, 1997, 100: 105–137
265 Liu Y B, Shao Y, Wang Y, et al. A multiple string matching algorithm for large-scale URL filtering. Chinese J Comput, 2014, 37: 1159–1169 [刘燕兵, 邵妍, 王勇, 等. 一种面向大规模 URL 过滤的多模式串匹配算法. 计算机学报, 2014, 37: 1159–1169]
266 Moulin P, Sullivan J A O. Information-theoretic analysis of information hiding. IEEE Trans Inform Theory, 2003, 49: 563–593
267 Du Q, Nekovei R. Implementation of real-time constrained linear discriminant analysis to remote sensing image classification. Pattern Recogn, 2005, 38: 459–471
268 Zhang L F. Algorithm for judging duplicate real-time packet in massive database. Comput Eng, 2008, 34: 76–80 [张立芳. 海量数据库中实时包的判重算法. 计算机工程, 2008, 34: 76–80]
269 Shahri H H, Shahri S H. Eliminating duplicates in information integration: an adaptive, Extensible Framework. IEEE Intell Syst, 2006, 21: 63–71
270 Liu Z, Zhao Z G. An Algorithm of Detection Duplicate Information Based on Segment. In: International Conference on Computational Aspects of Social Networks (CASoN), Taiyuan, 2010. 156–159
271 Heydon A, Najork M. Mercator: a scalable, extensible web crawler. World Wide Web-internet Web Inform Syst, 1999, 2: 219–229
272 Gautam P, Srinivasan P. Link contexts in classifier-guided topical crawlers. IEEE Trans Knowl Data Eng, 2006, 18: 107–122
273 Hai D, Hussain F K. Self-adaptive semantic focused crawler for mining services information discovery. IEEE Trans Ind Inform, 2014, 10: 1616–1626
274 Zhou D M, Li Z J. Survey of high-performance web crawler. Comput Sci, 2009, 36: 26–29 [周德懋, 李舟军. 高性能网络爬虫: 研究综述. 计算机科学, 2009, 36: 26–29]
275 Mladenic D. Feature Subset Selection in Text-Learning. Berlin: Springer, 1998. 95–100
276 Joachims T. Learning to Classify Text Using Support Vector Machines: Methods, Theory and Algorithms. Dordrecht: Kluwer Academic Publishers, 2002
277 Wang J. Digital audio watermarking algorithm based on modular arithmetic using DWT. Comput Eng, 2004, 30: 44–52 [王剑. 基于模数运算的 DWT 域数字音频水印. 计算机工程, 2004, 30: 44–52]
278 Barry A, Lee B F F. An audio delay system using digital technology. J Audio Engr Soc, 1971, 19: 393–397
279 Johnston J D. Transform coding of audio signals using perceptual noise criteria. IEEE J Select Areas Commun, 1988, 6: 314–323
280 Cinque L, Ciocca G, Levialdi S, et al. Color-based image retrieval using spatial-chromatic histograms. Image Vision Comput, 2001, 19: 979–986
281 Lu S W, Xu H. Textured image segmentation using autoregressive model and artificial neural network. Pattern Recogn, 1995, 28: 1807–1817
282 Gonzalez R C, Richard E. Woods, Digital Image Processing (3rd Edition). Upper Saddle River: Addison-Wesley, 2009
283 XU Z Z, Li J H, Yang S T, et al. A new robust content-based image authentication scheme. J Shanghai Jiaotong Univ, 2003, 37: 1757–1762 [须泽中, 李建华, 杨树堂, 等. 一种新的基于内容的稳健图像认证方法. 上海交通大学学报, 2003, 37: 1757–1762]
284 Song Y, Treanor D, Bulpitt A J, et al. Unsupervised content classification based nonrigid registration of differently stained histology images. IEEE Trans Biomedical Eng, 2014, 61: 96–108
285 Lu L, Zhang H J, Jiang H. Content analysis for audio classification and segmentation. IEEE Trans Speech Audio Process, 2002, 10: 504–516
286 Su G Y, Ma Y H, Li J H. One improved content based information filtering model. J Shanghai Jiaotong Univ, 2004, 38: 2030–2034 [苏贵洋, 马颖华, 李建华. 一种基于内容的信息过滤改进模型. 上海交通大学学报, 2004, 38: 2030–2034]
287 Hanani U, Shapira B, Shoval P. Information filtering: overview of issues, research and systems. User Model User-Adapted Interact, 2001, 11: 203–259
288 Nguyen V D, Varghese B, Barker A. The royal birth of 2013: analysing and visualising public sentiment in the UK using Twitter. In: IEEE International Conference on Big Data, Silicon Valley, 2013. 46–54
289 Tan S, Li Y, Sun H, et al. Interpreting the public sentiment variations on Twitter. IEEE Trans Knowl Data Eng, 2014, 26: 1158–1170
290 Li J H. Close attention to the importance of new applications of Internet content security management. Netinfo

Secur, 2008, 1: 23 [李建华. 密切关注互联网新型应用重视信息内容安全管理. 信息网络安全, 2008, 1: 23]

Survey on cyberspace security

Huanguo ZHANG[1*], Wenbao HAN[2], Xuejia LAI[3], Dongdai LIN[4], Jianfeng MA[5] & Jianhua LI[6]

1 *Computer School, Wuhan University, Wuhan* 430072*, China*;
2 *State Key Laboratory of Mathematics Engineering and Advanced Computing, Wuxi* 214122*, China*;
3 *Department of Computer, Shanghai Jiaotong University, Shanghai* 200240*, China*;
4 *Institute of Information Engineering, Beijing* 100093*, China*;
5 *School of Cyber Engineering, Xidian University, Xian* 710071*, China*;
6 *School of Information Security Engineering, Shanghai Jiaotong University, Shanghai* 200240*, China*
*E-mail: liss@whu.edu.cn

Abstract Along with the rapid development and wide application of information technology, human society is entering the information era. In this era, people live and work in cyberspace, which is a collection of all information systems, and the information environment for human survival. Therefore, ensuring cyberspace security is necessary. This paper provides a comprehensive introduction to the research and development, existing problems, and some popular research topics on the cyberspace concept, cyberspace security discipline, cryptography, network security, information system security, and information content security.

Keywords cyberspace security, information security, cryptography, network security, information system security, information content security

Huanguo ZHANG was born in June, 1945. He is a professor and Ph.D. director of the Computer School in Wuhan University. He graduated from Xidian University in July, 1970. His research interests include information security, cryptography, trusted computing, cloud computing, fault tolerance, and computer application.

Wenbao HAN is a professor at PLA information Engineering University. He obtained his Ph.D. degree from Sichuan University in 1994. He was a postdoctoral fellow at the University of Science and Technology in China, and a senior visiting scholar at CAS from 1997 to 1999. He visited the Mathematical Center of Obervolfach, Germany, in 2003. His research interest is computational number theory and cryptography.

Jianfeng MA was born in 1963. He received his Ph.D. degree from Xidian University, China, in 1995. He has been a professor in the Department of Computer Science and Technology, Xidian University, since 1998. He was the special engaged professor of the Yangtze River Scholar in China. Currently, he is the leader of the Shaanxi Key Laboratory of Network and System Security. His research interests include cryptology, network security, data security, and so on.

Jianhua LI is a professor and Ph.D. supervisor of the School of Information Security Engineering, Shanghai Jiao Tong University, Shanghai, China. He is also a dean in the same school. He obtained his B.S., M.S., and Ph.D. degrees from Shanghai Jiao Tong University, in 1986, 1991, and 1998, respectively. His research interests include information security, signal processing, computer network communication, etc.