中国科学 信息科学
SCIENTIA SINICA Informationis

网络空间安全体系与关键技术

罗军舟, 杨明, 凌振, 吴文甲 and 顾晓丹

Citation: 中国科学: 信息科学 **46**, 939 (2016); doi: 10.1360/N112016-00090

View online: http://engine.scichina.com/doi/10.1360/N112016-00090

View Table of Contents:http://engine.scichina.com/publisher/scp/journal/SSI/46/8

Published by the 《中国科学》杂志社

中国科学: 信息科学 2016 年 第 46 卷 第 8 期: 939–968
SCIENTIA SINICA Informationis
《中国科学》杂志社
SCIENCE CHINA PRESS
信息科学与技术若干前沿问题评述专刊

网络空间安全体系与关键技术

罗军舟*, 杨明, 凌振, 吴文甲, 顾晓丹

东南大学计算机科学与工程学院, 南京 211189
* 通信作者. E-mail: jluo@seu.edu.cn

收稿日期: 2016–04–09; 接受日期: 2016–06–17
国家自然科学基金 (批准号: 61320106007, 61272054, 61572130, 61502100, 61402104, 61532013) 资助项目

摘要 网络空间是一种包含互联网、通信网、物联网、工控网等信息基础设施, 并由人 – 机 – 物相互作用而形成的动态虚拟空间. 网络空间安全既涵盖包括人、机、物等实体在内的基础设施安全, 也涉及到其中产生、处理、传输、存储的各种信息数据的安全. 随着云计算、大数据、物联网、量子计算等新兴技术的迅猛发展, 网络空间安全面临着一系列新的威胁和挑战. 为此, 本文首先提出了 "四横一纵" 的网络空间安全研究体系, 涵盖物理层、系统层、网络层和数据层 4 个层面, 以及贯穿于上述 4 个层面的安全基础理论研究. 在此基础上, 着重阐述了需要重点布局和优先发展的若干基础理论和关键技术, 主要包括以下 6 个研究领域: 基于设备指纹、信道特征的硬件身份认证与安全通信, 云计算环境下的虚拟化安全分析和防御技术, 移动智能终端用户认证技术, 网络环境下的电力工业控制系统安全技术, 匿名通信和流量分析技术, 新密码体制基础理论与数据安全机制. 论文最后总结了网络空间安全研究领域未来的发展趋势.

关键词 网络空间安全 设备指纹 虚拟化安全 持续认证 工控系统安全 匿名通信 密码体制

1 引言

经过半个多世纪的发展, 以互联网为代表的计算机网络已经成为真正全球意义的信息共享与交互平台, 深刻地改变了人类社会政治、经济、军事、日常工作和生活的各个方面. 随着信息技术的持续变革推进, 计算机网络已不再局限于传统的机与机的互联, 而是不断趋向于物与物的互联、人与人的互联, 成为融合互联网、社会网络、移动互联网、物联网、工控网等在内的泛在网络.

鉴于传统的 "网络" 概念无法涵盖其泛在性及战略意义, 美国在 2001 年发布的《保护信息系统的国家计划》中首次提出了 "网络空间" (cyberspace) 的表述, 并在后续签署的国家安全 54 号总统令和国土安全 23 号总统令中对其进行了定义: "网络空间是连接各种信息技术基础设施的网络, 包括互联网、各种电信网、各种计算机系统、各类关键工业设施中的嵌入式处理器和控制器". 在国内, 沈昌祥院士指出网络空间已经成为继陆、海、空、天之后的第 5 大主权领域空间, 也是国际战略在军事领域的演进[1)]. 方滨兴院士 [1] 则提出: "网络空间是所有由可对外交换信息的电磁设备作为载体, 通过与人

1) http://news.xinhuanet.com/politics/2014-11/25/c_127250487.htm.

引用格式: 罗军舟, 杨明, 凌振, 等. 网络空间安全体系与关键技术. 中国科学: 信息科学, 2016, 46: 939–968, doi: 10.1360/N112016-00090

互动而形成的虚拟空间, 包括互联网、通信网、广电网、物联网、社交网络、计算系统、通信系统、控制系统等". 虽然定义有所区别, 但是研究人员普遍认可网络空间是一种包含互联网、通信网、物联网、工控网等信息基础设施, 并由人 – 机 – 物相互作用而形成的动态虚拟空间.

由于网络虚拟空间与物理世界呈现出不断融合、相互渗透的趋势, 网络空间的安全性不仅关系到人们的日常工作生活, 更对国家安全和国家发展具有重要的战略意义. 2012 年 12 月, 欧洲网络与信息安全局发布《国家网络空间安全战略: 制定和实施的实践指南》[2], 指出 "网络空间安全尚没有统一的定义, 与信息安全的概念存在重叠, 后者主要关注保护特定系统或组织内的信息的安全, 而网络空间安全则侧重于保护基础设施及关键信息基础设施 (critical information infrastructure) 所构成的网络". 而美国国家标准技术研究所在 2014 年发布的《增强关键基础设施网络空间安全框架》[3]对网络空间安全进行了定义, 即 "通过预防、检测和响应攻击, 保护信息的过程". 综合上述定义, 本文认为网络空间安全既涵盖包括人、机、物等实体在内的基础设施安全, 也涉及到其中产生、处理、传输、存储的各种信息数据的安全.

虽然网络空间安全已经得到普遍重视, 但近年来一些新的焦点问题相继显露, 例如: "伪基站" 导致的诈骗事件频频发生, 暴露了通信领域对物理接入安全的忽视; 云计算、大数据相关的新概念、新应用的不断出现, 使个人数据隐私泄露问题日益凸显; 计算和存储能力日益强大的移动智能终端承载了人们大量工作、生活相关的应用和数据, 急需切实可用的安全防护机制; 而互联网上匿名通信技术的滥用更是对网络监管、网络犯罪取证提出了严峻的挑战. 在国家层面, 危害网络空间安全的国际重大事件也是屡屡发生: 2010 年, 伊朗核电站的工业控制计算机系统受到震网病毒 (Stunxnet) 攻击, 导致核电站推迟发电; 2013 年, 美国棱镜计划被曝光, 表明自 2007 年起美国国家安全局 (NSA) 即开始实施绝密的电子监听计划, 通过直接进入美国网际网络公司的中心服务器挖掘数据、收集情报, 涉及到海量的个人聊天日志、存储的数据、语音通信、文件传输、个人社交网络数据. 上述种种安全事件的发生, 凸显了网络空间仍然面临着从物理安全、系统安全、网络安全到数据安全等各个层面的挑战, 迫切需要进行全面而系统化的安全基础理论和技术研究.

尤其是新型网络形态、新型计算基础理论和模式的出现, 以及信息化和工业化的深度融合, 给网络空间安全带来了新的威胁和挑战. 美国国家科学技术委员会在发布的《2016 年联邦网络安全研究和发展战略计划 — 网络与信息技术研发项目》[4]中指出, 物联网、云计算、高性能计算、自治系统、移动设备等领域中存在的安全问题将是新兴的研究热点. 同样, 鉴于网络空间安全所面临的严峻挑战, 2014 年 2 月我国成立了中央网络安全和信息化领导小组, 大力推进网络空间安全建设. 国务院学位委员会、教育部在 2015 年 6 月决定增设 "网络空间安全" 一级学科, 并于 2015 年 10 月决定增设 "网络空间安全" 一级学科博士学位授权点. 为了更好地布局和引导相关研究工作的开展, 国家自然科学基金委员会信息科学部选定 "网络空间安全的基础理论与关键技术" 为 "十三五" 期间十五个优先发展研究领域之一.

本文针对该优先研究领域涉及的各种安全理论和技术, 从物理层、系统层、网络层、数据层以及贯穿其中的安全基础理论的角度, 提出了 "四横一纵" 的网络空间安全研究体系, 并重点阐述了其中 6 个重要方向的研究现状和趋势, 具体包括: 涉及物理层接入安全和信道安全的基于设备指纹、信道特征的硬件身份认证与安全通信技术, 涉及系统层安全的云计算环境下的虚拟化安全分析、防御技术和

2) https://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/national-cyber-security-strategies-an-implementation-guide.

3) http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214-final.pdf.

4) https://www.whitehouse.gov/sites/whitehouse.gov/files/documents/2016_Federal_Cybersecurity_Research_and_Development_Stratgeic_Plan.pdf.

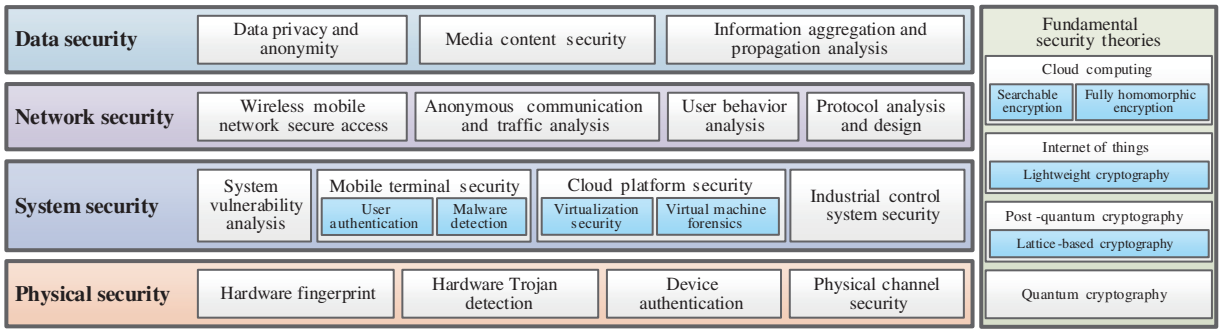

图 1 (网络版彩图) 安全研究层次体系及代表性研究方向

Figure 1 (Color online) Hierarchical security architecture and representative research areas

移动智能终端用户认证技术, 跨系统层、网络层的网络环境下的电力工业控制系统安全技术, 网络层的匿名通信和流量分析技术, 以及涉及数据层安全的新密码体制基础理论与数据安全机制.

2 网络空间安全研究体系

网络空间面临着从物理安全、系统安全、网络安全到数据安全等各个层面严峻的安全挑战, 因此有必要建立系统化的网络空间安全研究体系, 为相关研究工作提供框架性的指导, 并最终为建设、完善国家网络空间安全保障体系提供理论基础支撑.

为此, 国内学者纷纷开始探讨网络空间安全的内涵并梳理其中涉及的研究领域, 为构建网络空间安全研究体系提出了一些方案和建议. 方滨兴院士 [1] 提出了网络空间安全的 4 层次模型, 包括设备层的安全、系统层的安全、数据层的安全以及应用层的安全, 同时列出了信息安全、信息保密、信息对抗、云的安全、大数据、物联网安全、移动安全、可信计算 8 个研究领域, 并分析了这些领域在不同层面上面临的安全问题及对应的安全技术. 李晖等 [2] 则从学科人才培养的角度出发, 分析了网络空间安全学科与相关一级学科的关系, 并在此基础上提出了网络空间安全学科的 3 层知识体系, 其中底层是网络空间安全基础理论, 中间层包括物理安全、网络安全和系统安全, 顶层是数据与信息安全. 李建华等 [3] 指出网络空间安全是一门新兴的交叉学科, 包括网络空间安全基础、密码学及应用、系统安全、网络安全、应用安全 5 个研究方向, 其中安全基础为其他方向的研究提供理论、架构和方法学指导, 密码学及应用为系统安全、网络安全和应用安全提供密码机制.

在上述工作的基础上, 本文更多是从网络空间定义及其所涉及的实体, 而非网络本身的层次, 着手进行网络空间安全研究体系的探讨. 如前所述, 网络空间涉及到通过泛在网络连接在一起的人、计算机和各种物理设备, 其核心要素是在网络空间中产生、处理、传输、存储的信息数据 [2]. 与之相对应, 本文提出了如图 1 所示的 “四横一纵” 的层次化研究体系: 由于网络空间由各种物理设备组成, 物理层安全是网络空间安全的基础, 具体研究工作包括硬件指纹、硬件木马检测、设备认证、物理信道安全等; 物理设备的互联和通信需要相应系统的支持, 因此物理层之上为系统层安全, 主要关注系统脆弱性评估、移动终端安全 (包括用户认证、恶意软件识别等)、云平台安全 (包括虚拟化安全、虚拟机取证等) 和工业控制系统安全; 设备与设备之间的数据交换通过各类网络来进行, 因此系统层之上为网络层安全, 包括无线移动网络接入安全、匿名通信和流量分析、网络用户行为分析、网络协议分析与设计等研究内容; 网络空间中流动和存储的核心要素是信息数据, 而这些信息数据也是人在网络空

间中的具体映射, 因此该研究体系的最上层为数据层安全, 涉及数据隐私和匿名、媒体内容安全、信息聚集和传播分析等方面的研究工作; 而安全基础理论作为整个网络空间安全体系的基石, 贯穿于 4 层结构, 研究工作包括量子密码体制、后量子密码体制、面向物联网应用的轻量级密码算法和协议、云计算环境下支持密文统计分析的可搜索加密和全同态加密等方面的理论与方法. 5 个方面的具体论述如下所述.

1) 物理层安全: 主要研究针对各类硬件的恶意攻击和防御技术, 以及硬件设备在网络空间中的安全接入技术. 在恶意攻击和防御方面的主要研究热点有侧信道攻击、硬件木马检测方法和硬件信任基准等, 在设备接入安全方面主要研究基于设备指纹的身份认证、信道及设备指纹的测量与特征提取等. 此外, 物理层安全还包括容灾技术、可信硬件、电子防护技术、干扰屏蔽技术等.

2) 系统层安全: 包括系统软件安全、应用软件安全、体系结构安全等层面的研究内容, 并渗透到云计算、移动互联网、物联网、工控系统、嵌入式系统、智能计算等多个应用领域, 具体包括系统安全体系结构设计、系统脆弱性分析、软件的安全性分析, 智能终端的用户认证技术、恶意软件识别, 云计算环境下虚拟化安全分析和取证等重要研究方向. 同时, 智能制造与工业 4.0 战略提出后, 互联网与工业控制系统的融合已成为当前的主流趋势, 而其中工控系统的安全问题也日益凸显.

3) 网络层安全: 该层研究工作的主要目标是保证连接网络实体的中间网络自身的安全, 涉及各类无线通信网络、计算机网络、物联网、工控网等网络的安全协议、网络对抗攻防、安全管理、取证与追踪等方面的理论和技术. 随着智能终端技术的发展和移动互联网的普及, 移动与无线网络安全接入显得尤为重要. 而针对网络空间安全监管, 需要在网络层发现、阻断用户恶意行为, 重点研究高效、实用的匿名通信流量分析技术和网络用户行为分析技术.

4) 数据层安全: 数据层安全研究的主要目的是保证数据的机密性、完整性、不可否认性、匿名性等, 其研究热点已渗透到社会计算、多媒体计算、电子取证、云存储等多个应用领域, 具体包括数据隐私保护和匿名发布、数据的内在关联分析、网络环境下媒体内容安全、信息的聚集和传播分析、面向视频监控的内容分析、数据的访问控制等.

5) 安全基础理论和方法: 安全基础理论与方法既包括数论、博弈论、信息论、控制论、可计算性理论等共性基础理论, 也包括以密码学和访问控制为代表的安全领域特有的方法和技术手段. 在云计算环境下, 可搜索加密和全同态加密技术, 可以在保证数据机密性的同时支持密文的统计分析, 是云平台数据安全的一个重要研究方向. 在物联网应用中, 传感设备普遍存在着计算能力弱、存储空间小、能耗有限的特点, 不适宜应用传统密码算法, 这就使得轻量级密码算法成为解决物联网感知安全的基础手段. 同时, 为抵抗量子计算机攻击, 新兴的量子密码体制和后量子密码体制不可或缺. 这些研究工作为网络空间安全提供了理论基础与技术支撑.

简言之, 物理层安全主要关注网络空间中硬件设备、物理资源的安全, 系统层安全关注物理设备上承载的各类软件系统的安全, 网络层安全则保证物理实体之间交互的安全, 数据层安全是指网络空间中产生、处理、传输和存储的数据信息的安全. 此外, 还需要指出的是, 网络空间安全研究体系中涉及到的研究领域非常多, 图 1 仅是列举了一些具有代表性的热点研究方向, 而这些方向大部分也正是国家自然科学基金委 “十三五” 期间 “网络空间安全的基础理论与关键技术” 优先发展研究领域中所提及的内容, 其中 6 个方面的关键技术或理论将在下一节展开介绍.

3 若干重要研究方向

作为国家安全的重要组成部分, 网络空间安全对国际政治、经济、军事等方面的影响日益凸显, 迫

切需要对其进行全面而系统化的研究. 然而, 网络空间安全是一个覆盖面很广的综合性研究学科, 具体涉及的研究领域非常多, 本文仅对基于设备指纹、信道特征的硬件身份认证与安全通信, 云计算环境下的虚拟化安全分析和防御技术, 移动智能终端用户认证技术, 网络环境下的电力工业控制系统安全技术, 匿名通信和流量分析技术, 新密码体制基础理论与数据安全机制这 6 个重要方向的研究现状和趋势进行阐述.

上述 6 个研究方向既是目前的研究热点, 具有重要的理论意义和应用价值, 又涵盖了网络空间安全研究体系的各个层面, 具有足够的代表性和覆盖面: 基于设备指纹、信道特征的硬件身份认证与安全通信技术主要涉及物理层的接入安全和信道安全; 云计算环境下的虚拟化安全分析、防御技术和移动智能终端用户认证技术分别从不同应用领域的角度进行系统层安全的研究; 而网络环境下的电力工业控制系统安全技术则跨越了系统层和网络层两个层次, 用于保护智能电网的安全; 匿名通信和流量分析技术通过对匿名滥用的有效监管, 保护网络层的安全; 在数据层安全中, 本文重点关注抗量子新型密码, 以及适用于云计算和物联网领域数据安全保护的新型数据加密技术.

3.1 基于设备指纹、信道特征的硬件身份认证与安全通信

(1) 基于设备指纹的硬件身份认证

与生物学中人的指纹可用于身份认证类似, 在网络空间中接入的设备也具有其特有的 “指纹”, 可实现接入控制或者终端识别、追踪等目的. 传统上, 通常根据 MAC 地址、IP 地址等信息来标识网络设备, 但这些特征很容易被伪装、篡改, 因此设备指纹认证技术主要是通过收集设备的各种隐性特征来实现对其硬件身份的唯一识别, 如何选取识别精确度高、稳定性好的隐性特征是该研究领域的核心问题. 目前, 设备指纹认证技术主要分为基于瞬态特征、基于调制信号和基于内部传感器 3 类.

基于瞬态特征的设备指纹认证技术. 基于瞬态特征的设备指纹认证技术是指利用无线电信号开/关的瞬态特征来实现对设备的识别 [4]. 其基本流程为: 首先通过对瞬态信号的精确检测和隔离, 消除信号中的干扰因素, 然后抽取相关特征, 最后利用特征数据实现设备匹配. Tekbas 等 [5] 基于瞬态信号的振幅和相位变化值等特征研究环境因素对无线设备识别的影响. 该项工作利用概率神经网络对设备指纹进行分类, 通过对比实验发现了许多环境因素对设备识别有着显著的影响, 如电压值、周围温度等. 但是该工作必须在一个较大温差范围和电压变化范围内对设备指纹进行训练, 才能取得较高的识别率. Rasmussen 等 [6] 针对超高频传感器设备, 抽取瞬态信号的长度、振幅方差、载波信号峰值数、瞬态功率的标准化均值和最大值之间的差值以及离散小波变换系数等特征生成设备指纹向量, 并结合 Kalman 滤波技术对设备指纹进行分类和识别, 最终的实验结果取得了 70% 的识别率. 然而这类设备指纹的鲁棒性较弱, 当攻击者发送一个弱干扰信号时, 设备指纹将会发生显著的变化, 从而导致认证失败. Reising 等 [7] 针对 GSM 设备指纹技术进行研究, 他们从 GSM-GMSK (global system for mobile-Gaussian minimum shift keying) 突发信号中提取射频指纹, 利用最大似然估计和多重判别分析方法实现对设备的认证, 最终取得了 88%∼94% 的识别准确率.

基于调制信号的设备指纹认证技术. 基于调制信号的设备指纹认证技术主要是从调制信号中抽取特征以生成设备指纹, 从而对设备进行识别 [4]. Brik 等 [8] 利用无线网卡设备在制造工艺上的细微差异, 抽取无线网络帧在调制域中的相关特征生成设备指纹, 并借助机器学习算法实现了对设备的识别. 他们在 130 多个无线网卡上进行实验, 最终设备识别率高达 99%. Gerdes 等 [9] 发现不同厂商生产的有线网卡所产生的模拟信号是不同的, 从而提出了基于模拟信号的终端设备识别技术, 最多只需要 25 个数据帧就可以实现对终端设备的精确识别. 但是他们只是对低速网卡 (10 Mb) 进行了实验, 同时也没有考虑环境因素和设备的老化问题. 针对模拟信号和数字信号的差异, 该研究团队还提出了一种

新的基于硬件信号特征的设备指纹认证技术, 只需对一个物理帧进行特征抽取, 就能实现网卡设备的识别 [10]. Danev 等 [11] 将基于调制信号的设备指纹识别技术运用到对 RFID 设备的识别中, 并提出了多种方法实现设备指纹的提取. 通过抽取调制后的波形特征和频谱主成分分析特征, 利用最近邻算法和支持向量机分别对两类特征进行分类和识别, 最终实现了低于 5% 的误报率. 同时, 该项工作还针对电子护照进行了真实实验验证.

基于内部传感器的设备指纹认证技术. 基于内部传感器的设备指纹认证主要用于应用软件对智能终端的唯一性识别. 其基本思想是针对相同的外部刺激, 即使传感器属于相同品牌、相同型号, 由于制造工艺上的细微差别也会使它们获得/产生不同的传感数据. Dey 等 [12] 发现加速度传感器具有特殊的指纹, 可提取加速度传感器在时域和频域方面的 36 个特征生成设备指纹, 并利用 Bagged 决策树对指纹进行分类. 通过在 80 个加速度传感器芯片、25 台 Android 手机和 2 台 Android 平板电脑上进行实验, 其准确率和召回率均高达 96%. Bojinov 等[5)]分别利用扬声器和麦克风的音频频率响应和加速度传感器的校准误差实现对设备的识别, 其中加速度传感器指纹的获取仅是利用运行在 Web 浏览器中的 JavaScript 脚本, 而无需任何权限或用户干预. 实验结果表明传感器指纹能够在数千台设备中实现唯一的识别, 且冲突概率极低. Das 等 [13] 利用 Android 手机的扬声器和麦克风的声学特征进行设备识别, 但是该方法需要使用扬声器播放一些音乐, 隐蔽性较差. 而 Zhou 等 [14] 则根据扬声器对特殊频段音频的响应识别不同设备. 上述基于音频信号的设备指纹识别技术的准确率均易受到环境噪声的影响, 如何消除环境干扰有待进一步的研究.

(2) 基于无线信道特征的安全通信

早在 1949 年, Shannon 即指出只有实现 “一次一密” 才能达到绝对安全. 由于无线信道具有快速时变性, 即在时间间隔大于信道相干时间的情况下, 信道特征相互独立, 因此可利用无线信道特征来生成高安全性、低计算复杂度的密钥, 从而实现 “一次一密”, 保证通信的安全.

Maurer [15] 首先提出根据无线信道的互易性, 利用通信双方的公共信道特征生成密钥. 由于无线信道的空变性, 窃听者无法获得完整的信道特征, 因而无法生成和合法用户一致的密钥, 从而保证了密钥的安全. 由此可见, 基于无线信道特征的安全通信的核心是密钥的生成. 根据提取的信道特征的不同, 基于信道特征的密钥生成方法主要分为 3 大类: 基于接收信号强度 (received signal strength, RSS) 的密钥生成方法、基于信道相位 (channel phase) 的密钥生成方法和基于其他信道特征的密钥生成方法.

基于 RSS 的密钥生成方法. 由于 RSS 参数容易获取, 因此在密钥生成方法中得到了广泛的利用. Mathur 等 [16] 利用采样值的平均值和标准差来量化 RSS 参数, 从而提高了密钥一致率, 但是牺牲了密钥的生成速率. Jana 等 [17] 在此基础上提出了一种自适应的密钥生成机制, 将 RSS 序列分组量化, 并采用格雷码进行编码, 以此提高密钥的生成速率, 但是增加了密钥的不一致率. Patwari 等 [18] 提出了 HRUBE (high rate uncorrelated bit extraction) 机制, 利用多天线系统, 使用内插滤波法补偿通信双方信道测量误差, 并采用 KLT 变换 (Karhunen-Loeve transform) 去除测量值之间的相关性, 使得密钥生成速率和一致率均得到了提升. Liu 等 [19] 利用 RSS 参数提出了一种协作密钥生成机制, 实现了多设备通信的组密钥生成. 虽然 RSS 参数容易获取, 但信息较为粗略模糊, 密钥生成速率较低.

基于信道相位的密钥生成方法. 由于现有的信号处理技术可对接收信号进行高速率的分解评估, 因此基于信道相位的密钥生成方案可以高速率地生成密钥, 与基于 RSS 的密钥生成方法相比, 生成速率提高了至少一个数量级. 但是相位信息容易遭受噪音等干扰, 因而密钥的一致性较差. Yasukawa 等 [20] 首先利用离散余弦变换对信道相位信息进行预处理, 压缩冗余信息; 在此基础上, 实现信道相位

5) Bojinov H, Michalevsky Y, Nakibly G, et al. Mobile device identification via sensor fingerprinting. arXiv:1408.1416.

信息的多级量化并附加奇偶校验, 得到候选密钥集, 降低了密钥的不一致率. Sayeed 等 [21] 针对密钥协商后发现密钥不一致的问题, 研究密钥重传机制, 在重传时提高发射功率从而增加信噪比, 提高密钥一致率. Wang 等 [22] 则提出了一种在窄带多径衰落模型下利用信道相位信息生成密钥的方法, 可以支持高效的组密钥生成.

基于其他信道特征的密钥生成方法. 除了 RSS 和信道相位这两种常用的信道特征, 还有一些基于其他信道特征的密钥生成方案, 如信道状态信息 (channel state information, CSI)、信道脉冲响应 (channel impulse response, CIR) 等. Liu 等 [23] 提出一种基于 CSI 的密钥生成方法, 从 OFDM (orthogonal frequency division multiplexing) 的子载波中获取 CSI 生成密钥. 由于 CSI 提供了细粒度的信道信息, 降低了采样次数, 从而提高了密钥生成速率. 该方法还提出利用低密度奇偶校验码 (low-density parity-check code, LDPC) 调和双方生成的密钥, 提高密钥一致率. Chou 等 [24] 通过估计 CIR, 获取细粒度的信道信息来生成密钥, 提高密钥生成速率, 但是这种算法对硬件和能量的需求更高.

(3) 存在问题和未来发展趋势

基于设备指纹、信道特征的硬件身份认证与安全通信可以从以下 3 个方面开展进一步的工作: 1) 抗环境噪声干扰的设备指纹特征选取: 基于设备指纹的硬件身份认证依赖于提取的瞬态信号特征、调制信号特征、内部传感器数据等信息, 在实际应用中需要研究如何进一步去除环境中的噪声和干扰, 以获得准确的设备指纹特征信息. 2) 基于偏好、设置等应用层信息的设备指纹: 设备硬件指纹的研究集中在基于设备硬件差异的特征的提取, 而更上层的特征数据, 如浏览器插件、配置、历史信息和应用软件用户偏好、设置等也可用于生成设备指纹, 并且这类特征可以提高设备指纹识别的准确率. 3) 基于信道特征的一致性密钥的生成: 对于基于信道特征的密钥生成方法, 由于实际应用中上下行信道的不一致性、设备指纹以及测量中的误差等因素会造成信道特征提取的差异, 导致通信双方生成的密钥存在着不一致性. 因此, 需要研究密钥生成速率和一致性之间的权衡, 在保证密钥生成速率的同时, 降低密钥的不一致率.

3.2 云计算环境下的虚拟化安全分析和防御技术

当前, 云计算技术已被广泛地应用于各个领域, 包括城市管理、电子政务、园区服务、医疗卫生、教育、金融等. 云计算平台利用虚拟化技术共享计算资源, 改变了原来的计算模式, 提高了资源的利用率、灵活性和可用性, 但由于相同硬件资源承载了更多的计算任务, 其虚拟化技术自身的安全问题影响更为突出 [25]. 因此, 亚马逊、谷歌、微软、IBM 等国际大型 IT 公司均与著名大学合作, 开展云计算环境安全的研究. 同时, 美国国防预研计划局、美国国家科学基金会也加强了对云安全相关项目的资助. 本文主要针对云计算环境下的虚拟化安全分析和防御技术, 从攻击和防御两个角度阐述现有的研究工作.

(1) 云计算环境下虚拟机攻击技术

云计算环境下针对虚拟机 (virtual machine, VM) 的攻击可分内部攻击和外部攻击两类. 如图 2 所示, 攻击者可以通过虚拟机攻击虚拟机监控器 (virtual machine manager, VMM), 或者通过虚拟机管理工具攻击虚拟机监控器, 从而实现对同一宿主机上的其他虚拟机的攻击. 由于上述攻击是利用虚拟机内部漏洞发起, 可归为内部攻击. 此外, 攻击者还可以通过在宿主机安装 Rootkit 软件, 从而控制虚拟机监控器实现对整个虚拟机环境的攻击. 由于此类攻击是利用宿主机的漏洞从虚拟机外部发起, 称为外部攻击.

a) 虚拟机内部攻击

虚拟化的目标之一是通过隔离机制来保证虚拟机的安全, 而虚拟机内部攻击是破坏虚拟机的隔离

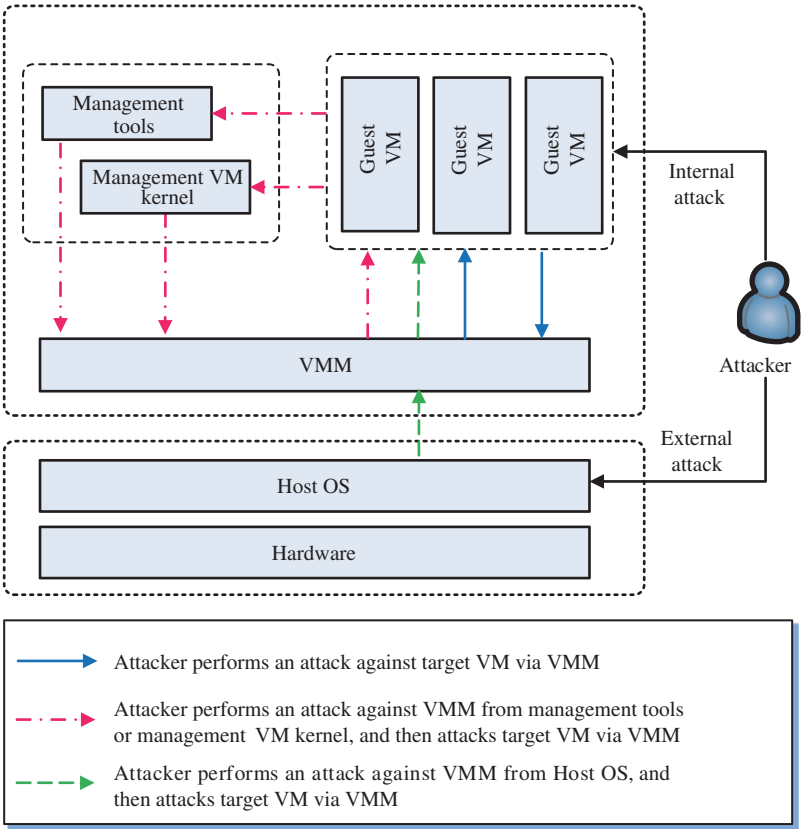

图 2 (网络版彩图) 云计算环境下虚拟机内部和外部攻击

Figure 2 (Color online) Internal attack and external attack against VM in cloud computing environment

性, 从而窃取同一物理主机中其他虚拟机用户的隐私和机密数据. 现有内部攻击方面的研究主要围绕攻击的三个步骤展开, 即虚拟机环境检测、虚拟机监控器识别以及破坏虚拟机的隔离性.

① 虚拟机环境检测: 虚拟化技术使得多个租户的虚拟机运行在一个独立的物理机上, 要攻击云计算环境下的虚拟机, 首先需要检测当前系统是否运行在虚拟机监控器之上, 从而判断目标机是否为虚拟机. Ferrie [26] 提出两种方法来检测虚拟机环境: 一是利用相同指令在物理机与虚拟机执行时长不同的特性进行判断, 通常虚拟机环境下执行指令的时间较长; 二是通过测算转译查找缓存 (translation lookaside buffers, TLB) 的存取时间来检测当前系统是否运行在虚拟机环境. 例如, 虚拟机敏感指令 CUPID, 若在虚拟环境中执行该指令, 虚拟机监控器将把部分 TLB 的数据页面清空, 导致这些数据页面访问未命中, 从而降低了数据读取速度. 利用这个特有现象, 当测量到 TLB 中缓存数据页面的访问时间较长时, 可判断 CUPID 指令是由虚拟机监控器执行, 从而断定当前运行在虚拟机环境中. 这两种方法均依赖于特定指令在不同环境下执行效果不同, 然而随着虚拟化技术的发展, 其中某些指令的执行效果已没有区分度.

② 虚拟机监控器识别: 在攻击者确定目标主机运行在虚拟机环境中之后, 将利用虚拟机监控器的特征或者漏洞来对虚拟机进行攻击. 而针对不同的虚拟机监控器需采用不同的攻击方式, 因此在攻击虚拟机之前, 需识别当前云计算平台部署的虚拟机监控器的具体类型. 有些特定的指令在虚拟机监控器和真实系统上的处理方式不同, 例如某些指令会导致监控器异常而真实系统则可正常运行, 反之亦

然. 利用这些特点, Ferrie 对 6 种类型的虚拟机监控器进行了识别 [26].

③ 虚拟机隔离性破坏: 虚拟机监控器保证了虚拟机之间的隔离性, 但它本身也存在漏洞. 当确定了虚拟机监控器的类型之后, 攻击者可以通过该监控器的漏洞或者错误配置对虚拟机系统发起攻击. 对虚拟机系统的攻击主要可以分为两种类型, 一是针对宿主机或该主机上其他虚拟机的攻击, 二是针对其他宿主机上虚拟机的攻击.

• **同一宿主机的虚拟机攻击.** 虚拟机监控器的主要目标就是保证租户虚拟机的隔离性, 如租户虚拟机不能获取超过其权限的资源. 然而, 攻击者可利用错误的虚拟机配置或设计缺陷破坏这种隔离性, 从而实现拒绝服务、系统挂起、虚拟机逃逸等攻击. 拒绝服务是指恶意虚拟机通过抢占宿主机的计算资源, 使其他虚拟机无法运行. Wojtczuk [6)]提出攻击者可通过修改 Xen 的代码和数据结构, 在虚拟机监控器或隐藏域内制造后门, 利用该后门可控制虚拟机监控器和虚拟机. 系统挂起是指攻击者通过精心设计的指令使虚拟机或虚拟机监控器挂起. 例如, 攻击者产生若干组随机指令序列并发送到不同类型的虚拟机监控器, 这些指令序列可能导致其挂起[7)]. 虚拟机逃逸是攻击者利用监控器源代码设计的漏洞获取最高权限, 并运行攻击者的恶意代码. 例如, 攻击者获取自身授权以外的内存访问权限, 执行恶意读写操作, 最终实现控制宿主机上其他虚拟机或虚拟机监控器的目的, 目前存在针对 Xen, VMWare [8)]和 Linux KVM [9)]的多种虚拟机逃逸攻击.

• **不同宿主机的虚拟机攻击.** 当攻击者控制了宿主物理机之后, 可以进一步对云中其他宿主机上的虚拟机发起攻击, 因此需要先确定目标虚拟机. 由于云环境中多个虚拟机共宿在同一物理机上, Ristenpart 等 [27] 提出一种隐蔽的方式来监控共宿虚拟机活动的方法, 该方法通过周期性地向云中虚拟机发送虚拟机之间基本的通信命令, 如查询 CPU 核数、存储容量等, 并根据响应时间来判断哪些虚拟机是在同一物理机上, 从而构建云环境中虚拟机的分布图. 然而, 该方法不能获取目标虚拟机行为相关的信息, 如缓存使用情况等.

b) 虚拟机外部攻击

在云计算环境中, 由于虚拟机均部署在物理机上, 攻击者可通过宿主物理机的攻击实现对其虚拟机的控制, 而这类攻击是从虚拟环境外部发起, 因此称为外部攻击. 此类方法主要基于虚拟机的隐匿技术攻击, 攻击者利用处理器的硬件辅助虚拟化技术在目标机系统上安装 Rootkit, 通过控制虚拟机监控器来控制整个虚拟机环境. King 等 [28] 提出在虚拟机运行过程中安装 Rootkit, 而 Rutkowska [10)]则提出在虚拟机重启过程中安装 Rootkit.

(2) 云计算环境下虚拟机防御技术

针对上述攻击, 现有的防御技术主要包括虚拟机安全监控、虚拟机隔离性保护和虚拟机监控器安全防护三个方面: 通过虚拟机监控, 发现对虚拟机系统的恶意攻击; 通过虚拟机隔离保护, 防止对虚拟机隔离性的攻击和破坏; 利用虚拟机监控器安全技术, 抵御来自虚拟机监控器的攻击.

a) 虚拟机监控

为实现虚拟机安全监控, 研究者们分别针对内、外部攻击, 提出了多种检测方法 [29~34], 其中比较典型的有虚拟机自省技术和 Rootkit 检测技术.

6) https://www.blackhat.com/presentations/bh-usa-08/Wojtczuk/BH_US_08_Wojtczuk_Subverting_the_Xen_Hypervisor.pdf.

7) http://taviso.decsystem.org/virtsec.pdf.

8) https://www.blackhat.com/presentations/bh-usa-09/KORTCHINSKY/BHUSA09-Kortchinsky-Cloudburst-SLIDES.pdf.

9) https://media.blackhat.com/bh-us-11/Elhage/BH_US_11_Elhage_Virtunoid_Slides.pdf.

10) https://www.blackhat.com/presentations/bh-usa-06/BH-US-06-Rutkowska.pdf.

虚拟机自省技术. 虚拟机自省技术是指通过虚拟机监控器访问虚拟机内存空间, 这样就可以在外部检测虚拟机中的数据, 并分析虚拟机的内容, 发现内部攻击. 根据分析结果, 可报告虚拟机异常或自动进行响应 [29]. Payne 等 [30] 提出了一种虚拟机自省方法, 通过将 hook 程序植入客户操作系统, 获取客户操作系统相关的较为全面的信息; 而 Ibrahim 等 [31] 则在没有获取客户操作系统相关信息的前提下, 通过重构不断变化的内核数据结构实现对租户虚拟机内存的实时监控. 上述方法虽然能保证虚拟机数据的安全, 但依然可能会泄露用户的隐私. 为了解决该问题, Yao 等 [32] 研究并设计了一种基于加密的虚拟机自省系统, 但是该系统依赖于应用层的加密机制, 系统效率有所降低.

Rootkit 检测技术. 由于外部攻击主要通过 Rootkit 实现, Rootkit 检测对于发现外部攻击至关重要. Seshadri 等 [33] 针对 Linux 内核研究并实现了一种检测系统 SecVisor, 只有用户确认的代码才可以在内核中执行, 可防御 Rootkit 等恶意代码的注入攻击. Litty 等 [34] 提出了一种 Rootkit 检测方法 Patagonix, 通过处理器硬件探测代码执行, 并依据可执行的二进制代码规范来识别代码, 同时验证代码是否被修改, 从而达到检测隐藏 Rootkit 的目的.

b) 虚拟机隔离性保护

虚拟机隔离性保护是指基于虚拟机监控器提供的安全模块, 使用强制接入控制技术在虚拟机间建立隔离. 因此, 虚拟机隔离性保护的本质是通过多租户访问控制技术实现虚拟机的隔离 [35].

Li 等 [36] 提出将云服务提供商和租户的安全职责分离, 并构建了一个基于多租户的访问控制模型. 该模型包含两个区组: 一个是用户区组, 用来划分 (隔离) 不同的租户; 另外一个是应用区组, 使租户自我管理对应用的访问. Tang 等 [37] 在多租户认证系统 (multi-tenancy authorization system, MTAS) 的基础上, 与基于角色的访问控制模型相结合, 提出了管理多租户认证系统 (administrative MTAS, AMTAS) 模型. 该模型在 MTAS 基础上增加了信任的条件, 对多租户之间的信任进行了形式化分析.

此外, 还可将访问控制策略部署在虚拟机监控器上, 通过集中部署访问控制策略来管理虚拟机监控器之上的所有虚拟机. Kurmus 等 [38] 分析了两种可有效实现多租户安全的架构, 即基于虚拟化和基于操作系统的多租户架构, 并证明了这两种架构都能在虚拟机监控器上隔离用户. Popa 等 [39] 提出了一种基于虚拟机监控器的多租户访问控制机制 CloudPolice. 该方法可让虚拟机监控器动态地协调虚拟机访问控制策略, 并根据源虚拟机到目的虚拟机之间的通信状况来确定访问控制策略的部署, 具体包括租户隔离、租户间通信、租户间公平共享服务和费率限制等.

c) 虚拟机监控器安全

对于来自虚拟机监控器的攻击, 现有的安全防护手段包括虚拟机监控器的安全防护、虚拟机监控器的权限控制、基于微内核的安全防护以及无虚拟机监控器架构.

虚拟机监控器的安全防护. 为防范来自虚拟机监控器的攻击, 保护其自身的安全至关重要. Azab 等 [40] 提出了 HyperSentry 框架, 可以避免被虚拟机监控器监控, 并通过系统管理模块进行隐蔽的上下文测量, 从而发现恶意虚拟机监控器的攻击路径. 该方法只能在攻击行为发生后恢复其攻击路径, 具有滞后性. 另一种方法 HyperSafe [41] 则是通过强制实施存储锁或限制检索, 增强虚拟机监控器的安全, 保证控制流的完整性.

虚拟机监控器的权限控制. 在云环境中, 虚拟机监控器拥有最高权限, 易被攻击者利用, 因此需要对其权限进行控制. 为此, Zhang 等 [42] 提出了基于 Xen 的 CloudVisor 原型系统, 该系统将监控器虚拟化并从特权区移除, 使其运行在 guest mode; 而 CloudVisor 则工作在 root mode, 虚拟机监控器对虚拟机的内存访问都将被其捕获.

基于微内核的安全防护. 该方法的思想是设计一种微内核作为虚拟机监控器, 使其只保留必备的功能. 由于微内核减弱了虚拟机监控器具备的能力, 从而降低了攻击者通过虚拟机监控器攻击虚拟机

的可能性. 此外, 微内核代码量少, 一旦出现问题, 也容易审查. Heiser 等 [43] 提出一种基于微内核的虚拟机监控器替代方案. Klein 等 [44] 则实现了微内核, 并证明了其安全性. Azab 等 [45] 提出基于 ARM 平台的微内核方案, 从而实现安全监控并保护内核不受更高权限软件的攻击.

无虚拟机监控器架构. 虚拟机监控器容易被攻击者控制, 是虚拟机安全的一个潜在隐患. 因此, 研究通过硬件辅助的虚拟化技术, 取消对虚拟机监控器的依赖, 可以从根本上消除这一隐患. 为此, Suh 等 [46] 提出了一种无虚拟机监控器的架构, 根据时间信道的固定划分来隔离同一物理机上的虚拟机. Xia 等 [47] 则提出移除整个系统的虚拟机监控器, 针对每台虚拟机创建相应的虚拟机监控器, 并通过虚拟机各自的监控器来保证整个系统的运行及虚拟机的隔离性和安全性.

(3) 存在问题和未来发展趋势

基于虚拟化的云计算技术在提高资源利用率的同时, 也引入了很多新的安全威胁. 尤其是针对虚拟机的攻击, 通过破坏其隔离性, 将导致数据泄露、拒绝服务等一系列的问题. 因此, 云计算环境下的虚拟化安全分析和防御技术可从以下几个方面做进一步研究: 1) 自主可控的虚拟化技术: 现阶段主要采用访问控制技术来保证虚拟机的隔离性, 但仅限于虚拟机监控器或虚拟机之间的访问控制, 还需研究两者结合的自主可控的虚拟化技术; 2) 针对虚拟机内部攻击的防御技术: 当前针对虚拟机的攻击主要包括内部攻击和外部攻击两类. 相较于外部攻击, 内部攻击的表现形式更为复杂多变, 因此针对内部攻击的防御技术是研究的重点. 考虑到内部攻击的本质是通过攻占虚拟机监控器来破坏虚拟机, 基于微内核的虚拟化技术将成为未来的主流解决方案之一.

3.3 移动智能终端用户认证技术

随着移动互联网的快速发展, 智能终端已逐渐成为网络攻击的目标, 对用户的隐私数据、线上资产等造成了极大的威胁. 而身份认证作为移动智能终端的第一道安全防线, 用于确保仅合法用户可访问系统, 其防护能力直接影响用户的信息安全. 依据认证事件发生时间的不同, 现有移动智能终端的认证技术可分为登录阶段的认证技术和会话期间的认证技术两类.

(1) 登录阶段的认证技术

登录阶段的认证技术在用户登录系统时验证用户身份, 系统依据认证结果授权或禁止用户访问. 依据认证过程中是否需要用户直接的物理性参与, 可以将其分为显式认证 (explicit authentication) 和隐式认证 (implicit authentication) 两类. 其中显式认证需要用户与设备直接交互, 如输入密码或验证指纹, 传统认证技术多为显式认证; 相反, 隐式认证的过程对用户透明, 不需用户显式执行指定操作.

a) 登录阶段的显式认证技术

由于传统的用户认证技术已在其他信息系统中得到广泛应用, 早期移动智能终端的用户认证技术也多采用传统方案实现, 主要包括基于知识的认证方案和基于令牌的认证方案. 基于知识的方案依赖于用户与系统之间事先协商的秘密信息 (如口令), 而基于令牌的方案则依赖于用户所持有的物品 (如 USB key). 随着移动智能终端内各种传感器的置入, 研究人员开始研究基于用户生物特征的认证技术.

基于知识和基于令牌的认证技术. 采用基于知识方案的认证技术主要有文本密码和图形密码. 常用的文本密码有 PIN 和字母数字密码: PIN 是一种纯数字密码, 用于在移动终端开机时对用户认证, 也用于保护 SIM 卡, 3 次错误输入会导致 SIM 卡锁定. 由于 PIN 码一般为 4~8 位数字, 密码空间较小, 易被攻击. 字母数字密码则是一种使用更为广泛的文本密码, 一般为字母、数字和符号组合, 易于更换, 在密码位数相同的情况下其密码空间较 PIN 更大. 但这类密码仍存在一些问题, 如增加用户的记忆负担, 进而导致用户选用弱密码、以明文方式写下密码或者为多个账户设置相同的密码等, 降低

了安全性. 此外, 文本密码还面临多种侧信道攻击威胁. 为了缓解此类威胁, 研究者提出了多种解决方案, 如针对文本密码易受计算机视觉攻击的问题, Ling 等 [48] 提出一种通过终端摄像头识别用户手指动作执行相应密文输入的技术, 并在映射用户手指运动的过程中加入了变速算法, 可有效抵御此类攻击. 但该方法受外界环境影响较大, 尤其是在光线较暗情况下对用户手指动作的识别准确率会大幅下降. 除了安全性问题之外, 文本密码还会增加用户记忆负担, 而相较于文本, 人类更善于记忆图像信息. 常见的图形密码认证方案主要包括 3 种实现形式: 绘制曲线连接特定图像、选中特定的图像或者选中图像中特定的点. 目前, Android 智能手机使用的图案锁屏就是一种图形密码方案, 用户通过在九宫格中绘制相应的图案作为图形密码进行认证, 但易受基于触摸屏残余物的攻击 [49] 或肩窥攻击. Gao 等 [50] 提出了一种可防御肩窥攻击的图形密码方案, 并且通过选用特定图片为用户构建故事场景降低用户记忆负担, 但存在用户难以区分不同退化图像的问题. Kwon 等 [51] 对图案锁屏进行改进以防御基于触摸屏残余物的攻击, 其基本思路为: 为基本的图案锁屏设置单独的输入区域, 用户在该区域内绘制解锁图案后, 通过执行额外的擦除操作涂抹之前的输入轨迹, 使其变得不可辨识. 但由于其需要用户执行额外的操作, 在一定程度上降低了系统的可用性. 当前移动智能终端平台在令牌认证方面的研究较少, 比较典型的如 Bojinov 等 [52] 研发的令牌设备. 基于对磁场信号和声音信号的调制, 他们分别设计了两种令牌设备, 当令牌设备处于终端一定范围内时, 便可实现认证. 总体而言, 基于知识和基于令牌的认证技术本质上是对用户持有物的认证, 而非对用户本身的认证.

基于用户生物特征的认证技术. 基于知识和基于令牌的认证技术通过验证用户所知道的秘密或所持有的物品实现对用户身份的认证. 严格来讲, 这些方案并不能验证用户本身的合法性, 而基于用户生物特征的认证技术可认为是对用户本身进行的认证. 生物特征识别是指利用个人具有的生理特征或行为特征来进行身份识别的一种技术. 其中, 生理特征多为先天性的, 如指纹、脸型、虹膜、掌纹、耳廓等; 而行为特征多为后天性的, 如步态、声纹、笔迹、击键行为特征等. Chen 等 [53] 提出一种利用移动智能终端内置的运动传感器来增强面部识别安全性的认证方案. Apple 公司在其 iPhone 5s 智能手机上开始应用指纹认证技术. 此外, 研究人员还根据用户皮肤纹路特征进行识别认证: Cheng 等 [54] 提出了一种基于用户指关节处皮肤纹路特征对用户进行认证的方案; Shabrina 等 [55] 提出了一种基于用户掌纹进行认证的方案; Raja 等 [56] 提出一种基于用户眼周生物特征信息来对用户进行认证的方案. 但此类认证技术通常仅进行了小范围的实验测试, 在现实场景下的可用性有待进一步研究验证.

b) 登录阶段的隐式认证技术

由于隐式认证技术在识别准确率和鲁棒性方面尚不能与传统认证技术相匹敌, 因此目前移动智能终端在登录阶段的认证多采用显式认证技术实现. 但基于知识和基于令牌的认证技术仅验证用户所知的秘密或所持有的令牌, 当密码或令牌被窃时系统的安全无法得到保障. 因而有学者提出在传统显式认证过程中对用户进行额外的隐式认证, 比较典型的如 de Luca 等 [57] 提出的认证方案: 在图案锁屏的基础上增加额外的、对用户透明的安全层, 根据用户输入的密文和输入操作过程中的行为特征对其进行认证, 主要包括触摸屏可检测到的触控坐标、压力、面积等, 即使密码被窃仍能在一定程度上保护用户的设备安全. 但该研究的实验样本较小且实验持续时间较短, 仍需进行更全面的实验以验证其实际可行性.

(2) 会话期间的认证技术

会话期间的认证技术是指在用户登录系统后的会话期间对用户进行认证, 从而弥补传统认证技术仅在登录阶段进行的不足, 形成对系统更完整的保护. 这类认证技术通常是一种持续认证, 即在一次授权会话期间重复性地验证用户身份的机制. 类似于登录阶段的认证, 会话期间的认证技术也包括显式认证和隐式认证. 但是, 由于在会话期间对用户进行显式认证会影响系统的用户体验, 因此通常使

用隐式认证的方式. 考虑到基于知识和基于令牌的方案较难实现透明认证, 而基于生理特征的方案存在一些限制, 如指纹识别技术需要特殊硬件支持且认证过程很难对用户透明, 因此目前主要采用基于行为特征的认证技术.

基于击键行为特征的认证技术. 早期的研究主要关注用户使用传统键盘时的击键行为, Clarke 等 [58] 的工作则是在移动设备上进行相关研究的代表. 随着配备触摸屏的移动智能终端的普及, 科研人员开始研究移动智能终端平台上基于软键盘使用行为特征的隐式认证的技术. Giuffrida 等 [59] 将击键过程中的时间特征与运动传感器信息结合, 利用标准的机器学习算法实现对用户的认证. 针对新型的手势键盘, Burgbacher 等 [60] 抽取用户使用手势键盘执行输入时的行为特征对短信息输入者的身份进行认证. 由于用户使用键盘与移动终端交互的频率不高且单次交互持续时间一般较短, 限制了该技术保护系统安全的能力.

基于步态的认证技术. 传统的步态识别主要利用图像和视频处理技术分析摄像头所录制的用户行走视频, 对设备计算能力要求高, 难以直接移植到移动智能终端平台. 但由于用户一般会随身携带移动智能终端, 设备内置的加速度传感器等可以用来检测用户行走过程中产生的振动. 在此基础上, 使用模式识别、机器学习等技术对传感器数据进行处理, 即可识别用户的步态, 从而达到对用户隐式认证的目的 [61].

基于触控行为特征的认证技术. 由于用户与移动智能终端的交互主要通过触摸屏进行, 利用该交互过程中用户行为特征进行认证的研究较多. Feng 等 [62] 重点关注用户多点触控操作时的行为特征, 提出了基于用户触控数据的认证方案. 考虑到单点的触控手势在交互过程中占比较高, Frank 等 [63] 从用户上下、左右滑动触控手势中提取行为特征进行认证. 由于用户的触控行为通常是一些简单的手指动作, 稳定性不足, 因此该方案目前尚不可独立地应用于较长时间跨度的用户认证, 通常作为锁屏的扩展或多模态生物特征认证系统的一部分. 针对触控行为模式易发生细微变化的问题, Shen 等 [64] 通过使用距离度量技术获得基于距离的本征空间 (distance-based eigenspace), 来缓解用户触控行为变化对认证产生的影响. 当前此类认证技术大多基于触摸屏可检测到的相关数据, 在识别准确率方面尚存提升空间, 未来可考虑综合使用多种传感器数据进行用户认证.

基于其他行为特征的认证技术. Jakobsson 等 [65] 针对移动智能终端用户的通话记录和位置轨迹模式进行了研究, 发现不同用户在一天的不同时段表现出不同的通话行为模式, 通过对用户位置轨迹信息的分析可识别出用户的居住、工作等地点, 从而在一定程度上区分不同的用户. 他们整合两个特征计算出一个总体的认证分数, 并基于预先设定的阈值实现对用户的隐式认证. 由于该方法基于对用户通话记录和位置轨迹的分析, 需收集较长时间的数据才能进行认证操作. 此外, Conti 等 [66] 利用移动智能终端的加速度和方向传感器, 提出了一种基于用户接听电话动作的隐式认证方案.

(3) 存在问题和未来发展趋势

在移动智能终端上, 认证技术被用来确保仅合法用户可访问系统资源, 是保障系统安全的第一道防线. 考虑到基于知识和基于令牌的认证技术本身存在固有缺陷, 基于用户生物特征的认证技术将是一个热点研究领域, 可从以下 3 个方面做进一步研究: 1) 多模态生物特征的应用: 现阶段, 使用单一生物特征的认证技术难以在安全性和可用性之间实现较好的平衡, 未来综合使用多种生物特征, 可进一步在不同场景下分别使用不同的生物特征组合, 保障安全性的同时兼顾可用性. 2) 用户行为特征模板的更新机制: 当前基于行为特征的认证方案大多未考虑用户行为可能随时间变化的情况, 系统鲁棒性较差, 未来需要对用户行为特征模板更新机制进行深入研究. 3) 生物特征模板数据的存储安全: 现有研究工作大多未考虑用户生物特征数据安全存储的问题, 如何安全存储用户的生物特征模板数据, 切实保障系统安全, 值得进一步深入研究.

3.4 网络环境下的电力工业控制系统安全技术

随着工业化与信息化进程的不断融合, 工业控制系统逐渐成为网络空间的一个重要组成部分, 并被广泛应用于能源行业、石油化工、水处理、交通、核工业等国家关键基础设施领域. 根据 2015 年美国工业控制系统网络应急响应小组的报告, 2014 年度工业控制系统安全事件的分布中能源行业比例达 32%, 这与以电力为主的能源行业对现实社会的重要性及其工控系统的自动化程度、信息化程度较高有紧密的关系, 因此对电力工业控制系统的攻击将带来巨大的经济损失, 甚至危害国家安全.

(1) 电力工业控制系统安全

目前, 面向电力工业控制系统的安全机制研究主要围绕智能电网开展, 在智能电表安全与隐私保护、智能电网数据采集与监控系统的攻击与防御等方面取得了一些研究成果.

a) 智能电表安全与隐私保护

为了提高智能电表终端的安全性, 研究者根据潜在的威胁模型, 提出了一些解决方案: McLaughlin 等 [67] 从攻击者的角度, 研究如何通过操纵高级量测体系 (advanced metering infrastructure, AMI) 系统来欺骗电网, 并对这种攻击的可行性进行验证, 从而发现现有 AMI 系统中存在多种能源窃取的途径. 为了防止攻击者伪造智能电表读数, Varodayan 等 [68] 提出了一种新的冗余测量机制来验证接收到的智能电表用户用电量读数, 从而保证其数据的完整性. Liu 等 [69] 针对 AMI 中的信息多混合传输模型、智能电表的信息存储和计算约束以及需求响应中参与者不固定 3 个问题, 提出一种新的密钥管理方案, 该方案基于密钥图技术, 采用密钥管理方法解决信息混合传输问题, 并采用加密和定期刷新两个策略解决后两个问题. Diao 等 [70] 提出一个基于 CL 签名的可链接匿名认证协议, 可以实现消息的身份认证和错误电表读数追溯功能. 该协议还具有不需要第三方认证、计算复杂度低和通信消耗低等特点.

为了保护智能电表的用户隐私, 研究者提出了相应的解决方案. Li 等 [71] 提出了一种分布式的增量数据聚合方案, 利用同态加密来保证数据在传输路径上的安全, 因此中间节点无法获取详细数据. Li 等 [72] 首次利用压缩感知技术上传智能电表数据, 实现传输速率的提升, 并使用随机序列来增强用户数据的隐私性和完整性. Rial 等 [73] 提出一种隐私保护协议用于分时电价计算, 应用零知识证明技术在不公开具体消费数据的情况下, 确保消费数据的正确性, 但是如何实现跨电网的数据聚集依然有待进一步的研究. Ruj 等 [74] 提出一个安全框架, 该框架将隐私数据聚集和访问控制进行整合, 利用同态加密保护用户隐私并利用基于属性的加密来保证访问控制的安全, 然而该方法中属性恢复过程会导致复杂的计算以及额外的通信负担. Rottondi 等 [75] 建立了一种隐私保护节点模型, 将测量数据聚集后再上传从而保证用户隐私信息. Birman 等 [76] 提出了一种数据收集方法, 利用差分隐私技术将电表中的聚合数据匿名化之后集中上传至数据中心, 并使用拜占庭容错算法在小部分电表被攻击的情况下也能保证整个系统的安全.

b) 数据采集与监控系统的攻击与防御

智能电网监控系统由大量布置的监控和测量设备组成, 监控和测量设备采集到的数据汇总到控制中心 (supervisory control and data acquisition, SCADA), 控制中心再根据这些数据评估电网状态. SCADA 的高效、安全运行依赖于设备数据的准确性和完整性, 通过注入虚假数据, 攻击者可以误导和操纵控制中心, 从而对整个电网造成严重危害 [77]. Liu 等 [78] 展示了一种新类型的攻击, 可以探测现存的虚假数据监测算法中的漏洞, 从而绕过系统的安全防护. Huang 等 [79] 从虚假数据攻击的角度进行研究, 提出攻击方可以进行独立组件分析, 在没有电网拓扑先验知识的情况下对电网拓扑进行推断, 并根据结果进一步发起攻击. Yu 等 [80] 利用主成分分析法在不知道电网拓扑信息的情况下达到隐秘

攻击的目的. 针对虚假数据注入攻击, 一些研究机构提出了相应的防御机制, 来保证状态评估的准确性. Bobba 等 [81] 提出一种监控系统防御机制, 通过加密足够数量的测量设备, 来保护状态评估系统不受隐秘攻击者的影响, 但是该机制的实施依赖于操作人员对被保护的传感器度量数据的实时获取. Dán 等 [82] 则拓展了上述研究工作, 提出了两种加密设备放置算法, 通过充分利用在系统中放置的加密设备来最大化整个系统的安全性. Liu 等 [83] 将虚假数据检测问题看成一个矩阵分离问题, 提出利用核范数最小化和低秩矩阵分解的方法对矩阵进行分离.

c) 信息传输安全

为了提高信息传输过程中的安全性与隐私性, 一些研究者提出了多种标准和防御措施. 美国国家标准与技术研究所指出, 网络不可用会导致无法实时监控关键电力设备和全局电力灾难, 所以鲁棒性是设计智能电网信息传输网络的首要标准. Lu 等 [84] 针对智能电网中通信网络面临的安全威胁进行分类评估, 基于自顶向下的分析, 将通信网络中潜在攻击分为网络可用性攻击、数据完整性攻击和隐私信息窃取 3 种类型, 并定性分析了这 3 种攻击的影响和可行性. Li 等 [85] 针对隐私信息窃取问题, 从信息论角度分析隐秘通信所需的信道容量, 提出了单电表情况下 Gauss 噪声通信信道方法. Khurana 等 [86] 提出一系列安全协议设计原则, 包括明确的节点名、统一编码、信任假设、时间戳、协议适用范围、机密公开、明确的安全参数等, 并讨论实际工程中如何确保智能电网身份认证协议的正确性和有效性.

(2) 存在问题和未来发展趋势

信息网络和工控网络的互联互通是未来发展的趋势. 工控系统安全研究跨越传统的工控系统和 IT 信息安全两个领域, 工控系统的安全脆弱性问题是因其重视工控系统的功能性实现、忽视安全性开发的历史原因造成的. 由于工控系统具有很高的领域专业性, 即使其安全脆弱性被发现, 但因缺乏相应的实验环境和领域知识, 难以采用传统意义上的信息安全技术及时处置. 因此, 工控系统信息安全研究是一个全新的战略发展方向.

具体在网络环境下的电力工业控制系统中, 有两个方面需要做进一步的研究: 1) 智能电表的防御技术: 在智能电网环境下, 针对智能电表的威胁种类较多, 如窃听、截取、伪造、重放、篡改数据, 渗透系统, 木马蠕虫病毒感染, 破坏物理链路, 分布式拒绝服务攻击等, 需要通过针对各种情况进行详细的研究, 才能有效地评估对智能电表的实际影响, 并进一步研究消除攻击威胁的防御措施. 2) 数据采集与监控系统的防御技术: 在数据采集与监控系统方面, 系统如果获取了恶意的电力数据并得出错误的状态估计值, 将导致工作人员做出错误的决策, 破坏整个电力系统. 因此需要针对各类潜在的数据采集与监控系统的威胁模型做进一步的研究, 并提出相应的防御措施.

3.5 匿名通信和流量分析技术

随着人们隐私保护意识的提高, OpenSSH, JAP, Tor, I2P 等低延时匿名通信系统相继出现并广泛应用. 然而, 随之而来的匿名滥用问题对网络空间安全造成了极大的威胁, 例如基于 Tor 建立的地下网络黑市 “丝绸之路” 提供了大量的毒品交易、军火买卖、黑客攻击等非法服务. 由于匿名通信系统对数据进行了加密处理, 在线破解这些密码算法难度较大且时间上不可接受, 因此流量分析技术成为最为有效的监管手段.

(1) 匿名通信系统

按照转发代理数量的不同, 匿名通信系统大致可分为单跳匿名通信系统和多跳匿名通信系统. 如图 3(a) 所示, 单跳匿名通信系统由用户、匿名服务器和应用服务器 3 部分组成: 用户通过匿名服务客户程序和匿名代理建立加密隧道, 由匿名代理将用户数据解密并转发给应用服务器. 应用服务器并不

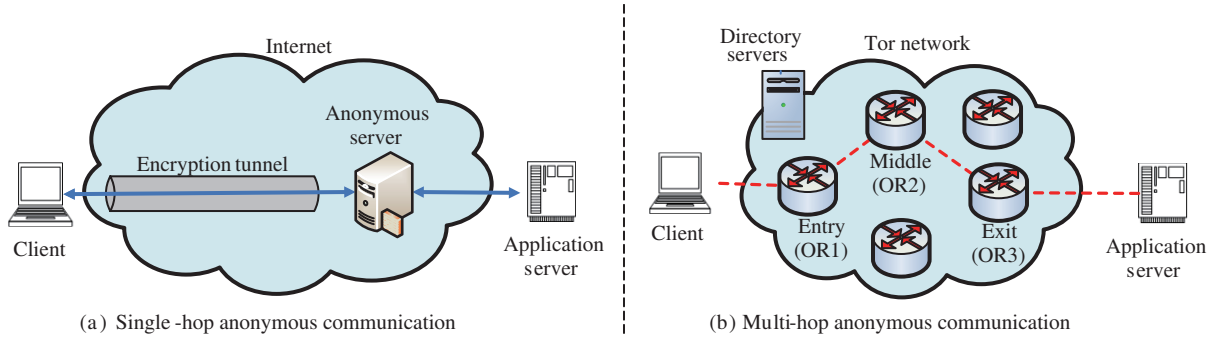

图 3 (网络版彩图) 匿名通信系统架构

Figure 3 (Color online) Anonymous communication models

知道用户真正的 IP, 只是将响应数据返回给匿名代理, 再由代理服务器返回给用户.

相对于单跳匿名通信系统, 多跳匿名通信系统的网络拓扑更为复杂, 协议更为完善. 目前使用最为广泛的多跳匿名系统 Tor 由用户端、OR (onion router) 节点、目录服务器和应用服务器 4 部分组成. 其中用户端从目录服务器处下载所有 OR 节点信息构建链路, 并将通信数据发送给本地 SOCKS 代理; OR 节点负责转发用户与应用服务器间的数据单元; 目录服务器负责收集所有 OR 节点信息; 应用服务器则为用户真正的通信目的地. 多跳匿名系统结构如图 3(b) 所示: 在通信时, 由客户端发起请求, 与每个 OR 节点分别协商生成密钥从而逐跳构建匿名电路. 然后, 客户端利用 TLS 加密链路传输已层层加密的数据, 并由每一跳节点分别解密, 最终在出口节点处以明文形式发送给应用服务器.

(2) 流量分析技术

流量分析是指通过嗅探并分析通信流量 (通常是加密流量) 的各种模式以获取有价值信息的一种技术. 从通信者的角度而言, 流量分析是一种针对通信匿名性的网络攻击行为, 但实际上该类技术被广泛地应用于网络监管和取证领域. 根据攻击者对通信行为的干涉程度, 可以将流量分析技术分为被动分析和主动分析两类: 被动流量分析是指通过被动网络窃听分析抽取流量特征的技术, 在这个过程中并不会影响数据的正常传输, 其优势在于隐蔽性强; 而主动流量分析则对数据通信过程本身施加干扰, 例如对数据包进行修改、重放、丢弃或延迟等操作, 从而达到更高效地进行流量特征分析和抽取的目的.

针对主动/被动流量分析, 根据威胁模型的不同, 又可以进一步分为端到端分析和单端分析两类: 同时占据通信入口和出口实施的流量分析称为端到端流量分析, 而仅占据发送端或接收端实施的流量分析被称为单端流量分析. 端到端流量分析的目的通常是进行通信关系确认, 在此类攻击中攻击者通过嗅探或干扰流量, 然后基于某些统计特征比对嫌疑发送端发出的流量和嫌疑接收端收到的流量, 一旦比对成功, 则可确认通信关系. 在单端流量分析中, 攻击者通常仅在发送端或者接收端对流量进行监控, 并从中提取特征构建流量模式. 下面将从被动/主动的端到端流量分析、被动/主动的单端流量分析 4 个方面 [87] 阐述现有相关工作.

a) 被动的端到端流量分析

在被动的端到端流量分析中, 攻击者仅监听通信流量, 根据嫌疑发送者的出流和接收者入流之间的相似性推断两者之间是否存在通信关系. 这种相似性一般通过提取流量本身的特征, 如报文个数、报文长度、时序关系等进行计算. 但是随着匿名网络规模的不断扩增, 攻击者同时监听到同一条链路上出口和入口流量的概率不断下降. 根据攻击者能力的不同, 现有被动端到端流量分析可以分为两种:

一种是攻击者为 AS/IX (autonomous systems/Internet exchange) 级别, 可以监听整个自治域或互联网交换中心内的信道; 另一种是攻击者向匿名通信网络注入节点, 通过一定策略增加自身被选中的概率, 从而实施攻击.

AS/IX 级别攻击. AS/IX 级别攻击是指攻击者可以在独立的自治系统或互联网交换中心级别对匿名链路进行监控分析, 从而实现通信关系的确认. 由于 Tor 现有的路径选择策略会尽可能使一条链路穿越不同的国家, 这就意味着即使是 AS/IX 级别攻击者也并不一定能同时监控出口和入口节点. 而 Edman 等 [88] 通过实验发现, 即使一条链路在地理位置上具有很大的跨度, 一般也只会穿过少数的 AS. 此外, 实验结果还显示一条匿名链路的入口和出口位置处于同一个自治域内的概率高达 22%. IX 具有比自治系统更大的监控范围, Murdoch 等 [89] 验证了 IX 级别攻击, 通过对真实的流量进行采样, 提取报文发送率、报文长度等统计特征, 实现了实体通信关系的确认. Johnson 等 [90] 在仿真环境下进行实验, 在同时控制具有高带宽的 Tor 节点以及互联网交换中心的条件下, 可以对 80% 的随机链路实现通信关系的确认. 在 AS/IX 级别攻击中, 攻击者需要对相当大范围的网络流量进行监控和分析, 这就对其所能掌控的资源有很高要求.

注入节点攻击. 注入节点攻击主要通过向网络中提供满足带宽、在线时间要求的恶意节点, 使其成为匿名系统的一部分来实施攻击. 而随着匿名网络规模的不断扩大, 受限于攻击成本, 攻击者无法提供足够的高带宽节点来获得更多链路的控制权, 因此需要采取一些措施提高注入节点被选中的概率. Bauer 等 [91] 提出了通过上传虚假高带宽信息提高恶意节点被选中概率的策略. Pappas 等 [92] 利用恶意用户节点构建环形链路, 恶意消耗链路中合法中继节点的资源, 最终使其资源耗尽拒绝服务, 从而间接提高恶意节点被选中的概率. 随着一些自动选取相对可靠中继节点的链路构建方案的提出, 注入节点攻击的有效性面临着更多的挑战.

b) 主动的端到端流量分析

在主动的端到端流量分析中, 攻击者通过操纵发送端或接收端的流量, 产生特定流量变化以注入信号, 然后在相应的位置对特定模式的信号进行恢复识别, 从而确认通信双方的通信关系. 根据实施层次的不同, 可以将这类攻击分为 3 种: 网络层流量分析、协议层流量分析和应用层流量分析.

网络层流量分析. 网络层流量分析通常利用目标流量的速率、报文间隔时间和报文大小等作为载体来嵌入标记信息, 从而实现通信关系的确认, 这类流量分析技术通常被称为网络流水印攻击. Yu 等 [93] 通过改变流量发送速率在发送方通信流中嵌入不同的秘密扩频标识, 该标识会随着通信流从发送方传播至接收方, 只需在接收方比对秘密扩频标识即可识别通信关系. Houmansadr 等 [94] 提出半盲的调制报文间隔的流水印机制, 使用扩频技术并在目标流量的报文间隔中加入极小的延时, 保证了攻击的隐蔽性, 成功在 SSH 流量上实施了攻击. Wang 等 [95] 设计时隙质心扩频水印机制, 以网络流时隙质心作为流水印的载体, 实现匿名网络下的跨域追踪. 在网络流水印研究领域, 如何进一步提高流水印的健壮性、如何平衡流水印的准确性和隐蔽性是重要的研究课题. 此外, SDN 软件定义网络的出现为网络流水印技术的部署提供了一个全新的平台, 这也是一个重要的新研究方向.

协议层流量分析. 协议层流量分析主要利用匿名协议的缺陷在流量中嵌入标记识别通信关系. Ling 等 [96] 通过控制 OR 节点并修改 Tor 协议, 在出口节点处连发 3 个 Tor 信元代表信号 1、1 个 Tor 信元代表信号 0, 并通过分析信元在网络逐跳传输中可能出现的变化, 设计信号恢复算法在入口节点处对信号进行识别, 可以在较短的时间内实现对 Tor 匿名流量通信关系的快速确认. 此外, Ling 等 [97] 还发现 Tor 系统中的每个节点都维护一个本地计数器来协调对收、发报文的加解密操作. 如果在入口节点处重放、删除或者加入一个报文, 导致中间节点和出口节点的计数值与入口节点不一致, 则报文在出口节点执行解密操作时就会发生错误. 一旦检测到这种错误, 就可以确定匿名通信关系. 针对

Anonymizer 匿名网络, Ling 等 [98] 提出在 Web 服务器和匿名代理之间通过调制报文长度嵌入信号, 并设计检测算法完成对信号的恢复识别.

应用层流量分析. 在应用层流量分析中, 攻击者主要通过在服务器返回给用户的 Web 响应流量中注入特定的内容, 使客户端流量产生可识别的模式特征. 一旦这种特征被占据入口节点的攻击者识别, 则通信关系确认. Wang 等 [99] 提出一种攻击方案, 在目标站点的流量中嵌入一个空对象, 使得用户端在收到响应流量后去请求该空对象并产生相应的流量特征, 通过流量特征的匹配可以确认通信关系. Chakravarty 等 [100] 在 Web 服务器端加入代码让用户下载一个较大且不易被察觉的文件, 然后根据统计相关性在收集到的众多入口 NetFlow 流量记录中找到符合此流量特征的入口节点, 从而确认通信关系. 此类的攻击还可以通过在用户的返回流量中注入 JavaScript 代码来触发用户端浏览器产生特定的信号流量.

c) 被动的单端流量分析

被动的单端流量分析技术主要是指 Web 站点指纹攻击. 在 Web 站点指纹攻击中, 攻击者使用匿名代理模拟用户行为访问站点, 对获取的流量提取特征形成站点指纹并建立 Web 站点指纹库, 然后对用户的在线匿名流量提取特征形成用户指纹, 通过将用户指纹与指纹库中的指纹进行对比, 从而识别出用户访问的站点.

Hintz [101] 最先提出了 Web 站点指纹攻击的概念, 并在理论上证明了指纹攻击的可行性与有效性, 但该攻击方案仅适用于 HTTP1.0 协议, 对之后的 HTTP 协议不再有效. Liberatore 等 [102] 在前人工作的基础上, 仅使用报文长度分布为特征, 首次将机器学习领域的朴素 Bayes 分类器应用于指纹识别, 大大提高了单跳匿名代理上指纹攻击的成功率. 但该方案依赖于上下行流量中报文的长度, 并不适用于对报文进行了定长封装处理的 Tor 等多跳匿名通信系统, 具有较大的局限性, 并且忽略了流量中报文方向这一关键特征. Panchenko 等 [103] 通过综合多种流量特征, 包括特定长度报文出现次数、总传输量、上下行报文数据量及所占比例等, 并使用支持向量机 (support vector machine, SVM) 对指纹进行分类, 将多跳匿名代理上的识别率从 3% 提升至 55%. Cai 等 [104] 针对 Tor 信元定长封装的特性对报文长度进行处理, 并使用最佳字符串编辑距离 (optimal string alignment distance, OSAD) 为 SVM 的核函数衡量指纹相似性, 在 Tor 上取得较好攻击效果. Wang 等 [105] 在 Cai 等的研究基础上将特征集扩大, 调整不同特征所占权重, 使用 K 近邻作为分类器, 降低了计算成本, 攻击效果进一步提升. 然而, Web 站点指纹攻击的实施依赖于一系列假设, 如用户浏览器关闭了缓存功能、用户浏览网页过程中较少出现背景流量等, 消除这些假设对于方法的实用性具有重要的意义.

d) 主动的单端流量分析

主动的单端流量分析可以在两处位置实施, 一种是在出口节点与应用服务器间的未加密链路上注入恶意代码, 另一种是控制用户的入口节点或链路执行主动 Web 站点指纹攻击.

注入恶意代码. 当攻击者控制了应用服务器端的未加密流量时, 可以将 Flash ActionScript, JavaScript, ActiveX 等恶意代码注入到返回流量中. 当这些代码到达用户端并被浏览器执行时, 会导致浏览器绕过本地设置不使用加密代理, 而是直接与远程服务器建立连接, 从而暴露真实的 IP 地址.

主动 Web 站点指纹攻击. 在被动的 Web 指纹攻击中, 攻击者仅监听链路, 并不会对流量进行主动调制. 由于 Tor 等匿名通信系统的定长封装机制和 HTTP 持久连接、流水线等技术的影响, Web 页面不同对象的数据在返回流量中出现重叠难以区分, 导致指纹攻击的正确率无法进一步提升. 如果可以采取某些方法使不同对象的返回流量区分开来, 则可以更好地为不同 Web 站点建立指纹. He 等 [106] 首次提出并针对 Tor 系统进行了主动 Web 站点指纹攻击, 通过对 Tor 流量进行观察确定用户开始发送请求报文的位置, 然后主动延迟用户发出的请求报文, 使前一个请求对象的响应数据有足够

时间完成传输, 从而达到分离不同对象流量的目的. 然而该攻击会造成报文重传, 隐蔽性较差, 并且延迟操作的粒度较粗, 未对上行流量中存在的大量匿名协议控制报文进行识别.

(3) 存在问题和未来发展趋势

随着各类匿名通信系统的广泛部署和应用, 加密流量、匿名流量在网络流量中所占的比例呈现出快速增长的趋势, 因此采用流量分析技术实现对这部分流量的识别、分析和追踪, 从而加强针对整个网络空间的监管是必然的趋势. 现有研究工作可以从以下几个方面推进: 1) 大规模数据报文的高速处理: 针对动态实时到达的大规模数据报文流量, 需要设计面向流式大数据处理的增量计算模型, 研究流自适应的内存管理优化方法, 支持快速、高效的大规模数据报文处理与分析. 2) 基于压缩感知的流量模式统计分析: 设计面向高速环境网络数据流的压缩和统计信息抽取方法, 基于压缩感知理论, 在满足严格的存储空间约束的前提下, 设计支持海量数据流并行处理的分析算法, 并将传统的流式数据处理拓展到对整个时间轴网络行为的监测, 挖掘跨越多个时间段的持久流量模式特征. 3) 加密网络流量的识别和分析: 进一步开展加密流量识别、应用分类和内容分析核心算法的研究. 利用挖掘出的网络数据流量模式特征, 设计增量式算法, 以实现快速、高效的匿名通信流量识别和应用分类. 针对 HTTP 等典型匿名通信流量, 设计主动流量分析技术以推测潜在的通信目标.

3.6 新密码体制基础理论与数据安全机制

密码技术是保障网络空间安全的基本手段. 多年来, 国内外研究人员不断研究推动密码技术的发展. 尤其是物联网、云计算、大数据等新型网络形态和服务的兴起, 数据安全共享与隐私保护之间的冲突渐增, 再加上量子计算对现有计算能力的革新, 使基于大整数分解和离散对数的密码体制将不能保证安全性, 密码技术迎来了新的挑战. 为了应对这些挑战, 抗量子密码、全同态加密、可搜索加密、轻量级加密等新兴技术相继被提出.

(1) 抗量子密码

量子计算机的诞生及其量子位数的提升证明了量子计算机原理的正确性和可行性. 得益于量子计算机的高速计算能力, 科研人员已经研究出能够有效解决离散对数和因子分解的量子算法, 这就意味着许多经典加密算法 (如 RSA) 已经无法保证信息的安全有效. 为了应对量子计算给现行密码体制带来的挑战, 学者们提出了 “抗量子密码” 的概念. 目前, 抗量子密码主要包括量子密码、基于数学问题构建的经典抗量子密码等.

a) 量子密码

量子密码是以量子态为符号实现的密码, 其基本思路是利用光子传送密钥信息. 相较于传统的密码技术, 以 “海森堡测不准” 和 “量子不可克隆” 原理为基础的量子密码体制在理论上具有 “无条件安全性”, 即当输运光子的线路遭到窃听时, 会破坏原通信线路之间的相互关系, 导致通信中断. 目前, 研究人员对量子密码的研究涉及量子认证、量子密钥管理、量子密码分析等多个问题, 其中量子密钥分配仍然是主要的研究方向.

早在 20 世纪 70 年代, “量子密码” 的概念就被提出. 1984 年, Bennett 和 Brassard [107] 提出了量子密钥分配概念和 BB84 协议, 证明了量子密码技术的可行性. 在此基础上, Lo 等 [108] 最早在理论上给出了 BB84 协议的无条件安全分析. 1990 年后, 量子密码得到了人们的青睐与重视, 迅速地发展起来. Ekert [109] 提出了基于双量子纠缠的协议 EPR (Einstein Podolsky Rosen). Bennett [110] 又提出了 B92 协议, 该方案较之 BB84 更简单, 但是效率减半, 实际应用时在高损信道上存在安全隐患. 至此, 3 大主流量子密钥分发方案基本形成.

近 20 年, 国内外科研人员对量子密钥的分发进行了许多实验研究. 美国、欧盟和日本很早就投入了大量的资源进行量子密码通信网络的建设, 而我国在量子密码领域也取得了诸多研究成果. 2005 年, 潘建伟研究组发表了关于 13 公里自由空间纠缠光子分发的研究成果 [111], 验证了在地球与外层空间之间分发纠缠光子的可行性. 为了克服不完美光源带来的安全漏洞, 提高量子密钥分发的安全距离, 他们还提出并实现了诱骗态通信技术 [112]. 到 2009 年, 中国科学技术大学与清华大学的联合小组成功实现了 16 公里的自由空间量子态隐形传输, 证实了自由空间远距离量子隐形传输的可行性 [113].

b) 经典抗量子密码

现有的经典抗量子密码研究主要集中在 Merkle 认证树签名、基于纠错码的公钥密码、基于格的公钥密码和 MQ 公钥密码几个方面, 其中基于格的公钥密码体制的研究相对成熟. 基于格的密码体制是指基于格困难问题及其变种而建立起来的一系列密码方案, 常见的格问题主要包括最短向量问题、最近向量问题、小整数解问题和误差学习等. 虽然量子算法可以破解许多经典加密算法, 但到目前为止还不能有效解决格困难问题. 另外, 格困难问题都是基于最坏情况假设的, 这就意味着基于格的密码方案可以被规约为最坏情况下的格困难问题, 从而保证了这类加密方案的安全性.

基于格的突破性研究开始于 AD 公钥密码方案, 虽然该方案具有良好的安全性, 但实现效率较低, 缺乏实用性. 随后, 其他基于格的密码方案被相继提出: 1998 年, Hoffstein 等 [114] 提出了一种在环上构建的公钥加密方案 NTRU (number theory research unit), 该方案可以使用一种特殊结构的格来描述, 大大提高了加密效率, 但存在解密错误问题, 也没有在理论上证明其安全性. 2005 年, Regev [115] 设计了一种基于格误差学习 (learning with error, LWE) 的单比特公钥加密方案, 但仍存在效率低下的问题. 为了提高 LWE 的效率, 解决实用性问题, 又有许多学者对此进行了改进. 2009 年, 基于理想格的全同态加密方案被提出 [116], 允许直接对密文进行使用和分析, 因此可以将其应用于云计算领域, 解决数据安全问题. 2010 年, Agrawal 等 [117] 构造了一个基于双陷门单向函数的 HIBE (hierarchical identity based encryption) 方案并给出了方案的安全性证明. 此后, 新兴的盆景树技术为格提供了良好的基扩展、基变换和基随机化方法, 使基于格的代理签名成为可能. 2012 年, Lyubashevsky [118] 提出了一种基于拒绝采样算法的数字签名方案, 大大提高了基于格的数字签名方案的实用性.

此外, 以 DNA 作为信息载体的 DNA 密码也是抗量子密码算法设计的一种有效途径. 1994 年, Aldeman [119] 首次使用现代分子技术解决 NP 问题后, DNA 计算开始得到科研人员的关注, 而 DNA 密码就是伴随 DNA 计算的研究而出现的密码技术. 目前科研人员针对 DNA 密码的研究主要有 3 个研究方向: DNA 隐写技术、DNA 认证技术和 DNA 加密技术. 相较于传统密码, 利用现代生物技术的 DNA 密码具有高度并行性, 加、解密速度快. 另外, 因为 DNA 密码建立在 DNA 分子基础上, 具有高密度性, 其安全性不完全依赖于困难的数学问题, 所以不易破解, 具有巨大的发展潜力. 但是 DNA 密码技术理论目前尚不够成熟, 体系不完整, 实现较为困难.

(2) 面向云环境的密码技术

云环境给用户带来计算资源和存储资源的同时, 也面临着数据机密性、访问可控性、数据完整性和隐私性等方面的严重安全威胁 [120]. 本文重点关注与数据机密性和访问可控性相关的新兴密码技术, 包括全同态加密、可搜索加密和功能加密.

a) 全同态加密

同态加密是一种新的加密机制, 它对明文进行加法或乘法运算后加密的结果与对密文进行相应运算之后的结果等价, 同时满足加同态和乘同态的同态加密叫作全同态加密. 在云平台中, 利用全同态加密算法对用户数据进行加密上传后, 数据使用者在不解密的情况下, 仍可对这些数据进行分析使用, 在一定程度上解决了云环境中的隐私安全问题, 因此全同态加密成为国内外密码学界研究的热点. 早

在 1978 年, 继提出 RSA 之后, Rivest 等 [121] 就提出了同态加密的概念, 但其作为一个公开问题一直未能得到解决. 直到 2009 年 Gentry [116] 首次提出基于理想格的全同态加密机制后, 全同态加密才逐渐发展起来. 因为该方案效率不能满足实际应用的需求, Dijk 等 [122] 在其基础上, 提出了更简洁的基于整数的全同态加密机制, 安全性基于近似最大公约数. 近年来, 全同态加密在算法改进和实用化方面得到了进一步的发展, 算法大多基于 LWE 问题和环 -LWE 问题, 安全性较高.

b) 可搜索加密

在云环境下, 用户希望数据在云端既是加密的, 又能够直接从密文中搜索到所需内容, 而不需要对数据下载解密. 作为一种允许用户在密文中进行关键字查询的加密技术, 可搜索加密技术在这样的环境下应运而生. 目前, 依据构造算法的不同, 可搜索加密机制主要分为基于对称密钥和基于公钥两类. 2000 年, Song 等 [123] 最早提出了在密文上进行搜索的实现方法, 该方法基于对称密钥, 但效率较低, 安全性也不够高. 2004 年, Boneh 等 [124] 首次提出了支持加密搜索的公钥密码体制, 将可搜索加密从对称密钥扩展到公钥体制. 之后, 为了改善可搜索加密机制的性能、提升用户的搜索体验, 许多研究人员对可搜索加密进行理论扩展并尝试将其投入实际应用 [125], 可搜索加密机制从仅支持单词搜索, 逐渐发展到支持多词搜索、支持连接关键词搜索、支持排序搜索和复杂的查询, 加密模型也从 “一对一” 的单方模式发展到 “一对多”、“多对一” 和 “多对多” 的多方模式.

c) 功能加密

功能加密是一种支持在密文条件下对其进行计算和对不同数据使用者分配不同解密权限的加密技术, 基于身份加密、基于属性加密和谓词加密都可以被认为是功能加密的分支. 功能加密支持灵活的密文解密表达式, 可以给不同数据使用者分配不同的权限, 很大程度上丰富了信息的共享方式, 在云环境中具有很高的实用性. 功能加密最早可以追溯到 2005 年 Sahai 等 [126] 在欧洲密码学年会上提出的模糊身份加密. 2010 年, 同样是在欧洲密码学年会上, Lewko 等 [127] 首次提出了 “功能加密” 概念. 同年, O’Neill [128] 提出了功能加密的通用框架. 2011 年, Boneh 等 [129] 也给出了关于 “功能加密” 的通用解释. 近年来, 众多研究者围绕功能加密, 尤其是在基于属性加密方面, 进行了理论扩展和实践应用等多方面的研究 [130].

(3) 面向物联网环境的轻量级密码技术

随着物联网技术的快速发展, RFID 标签、智能卡、无线传感器等低能耗嵌入式智能设备受到越来越多的关注. 由于这些设备的计算能力、存储空间和能量来源有限, 如何设计适用于资源受限设备的轻量级密码技术逐渐成为研究热点. 目前, 轻量级密码体制主要分为轻量级对称密码、非对称密码和 Hash 函数等.

a) 轻量级对称密码技术

轻量级对称密码技术可分为分组密码和流密码, 其中分组密码是迄今为止最为成熟的一种轻量级密码, 它在硬件、加密效率和功耗等方面都具有明显优势. 目前主要的研究工作集中于对标准和典型分组密码的优化以及全新轻量级密码的设计. 轻量级流密码结构比较简单, 加解密效率也很高, 所以也是当前的研究热点. 但是流密码在初次使用时需要漫长的初始化阶段, 而且有一些通信协议并不支持流密码. 因此, 相比于分组密码, 流密码的设计技术还不够成熟. 目前比较流行的流密码有 2004 年欧洲 eSTREAM 计划提出的 Salsa, Grain, TRIVIUM 方案和 2011 年 David 等 [131] 提出的专用轻量级密码方案 A2U2.

b) 轻量级非对称密码技术

相较于对称密码, 轻量级非对称密码技术具有一定的优势, 设备之间可以仅采用单方的公钥即可实现认证、加密等功能, 可以避免复杂的密钥管理和分配工作. 但是公钥加密算法本身比较复杂, 设

计轻量级非对称密码算法就显得更为困难, 目前该领域的研究工作尚处于起步阶段. Saarinen [132] 在2012 年提出了基于 Rabin 的混合公钥加密机制 BlueJay, 采用了随机数乘法技术, 避免了大整数计算, 提高了加密效率. 另外, 椭圆曲线加密具有加密效率高、占用存储空间小等优点, 在实现轻量级非对称密码方面也有较好的发展前景.

c) 轻量级 Hash 函数

传统的 Hash 函数包括 MD5 和 SHA 等, 但这些都不适用于资源受限的设备. 因此, 设计适用于资源受限设备的轻量级 Hash 函数也成为了研究热点. 目前, 根据迭代压缩函数的不同设计原理, 轻量级 Hash 函数主要分为以下 3 类: 基于置换函数的轻量级 Hash 函数、基于分组密码的轻量级 Hash 函数和基于数学困难性问题的轻量级 Hash 函数 [133].

基于置换函数的轻量级 Hash 函数. 2011 年, Bogdanov 等 [134] 采用类似于 PRESENT 轻量级分组密码的置换函数, 设计出轻量级 Hash 函数 SPONGENT. 2012 年, Keccak 方案最终成为 SHA-3 竞赛的获胜者, 证明了在内存开销方面, 基于 Sponge 结构的 Hash 函数具有明显的优势.

基于分组密码的轻量级 Hash 函数. 2007 年, Yoshida 等 [135] 基于 Type-1 4-Branch 广义 Feistel 结构的轻量级分组密码提出轻量级压缩函数 MAME, 在硬件开销上具有优势. 2010 年, Hirose 等 [136] 提出轻量级 Hash 函数 Lesamnta-LW, 其设计方案也采用了 Fesitel 广义结构, 其构造方法要求分组长度是密钥长度的两倍. 但实际上密钥长度大于分组长度, 为了解决该问题, Kuwakado 和 Hirose [137] 提出 KH 构造方法.

基于数学困难性问题的轻量级 Hash 函数. 2007 年, Billet 等 [138] 提出了基于多变量非线性方程组的 Hash 函数, 相比于传统的基于数学困难性问题的 Hash 函数, 该方案在性能和实现开销方面具有明显的优势. 此外, 研究人员还认为使用稀疏的多变量非线性方程组能进一步提高性能, 降低开销. 而 Bettale 等 [139] 则认为此类方案的安全性太低, 无法在实际中应用, 并在理论上给出了计算复杂度分析. 目前, 基于数学困难性问题的轻量级 Hash 函数虽然存在一定的可行性, 但是实现代价太大, 难以得到实际应用.

(4) 存在问题和未来发展趋势

密码技术的研究主要涉及到密码算法的设计、分析与应用. 为了应对量子计算、云计算和物联网等新的计算资源和新的服务形式带来的问题和挑战, 抗量子密码、云环境下的新兴密码和物联网中的轻量级密码逐渐成为密码技术的研究热点: 1) 量子密码理论、技术的进一步完善: 在抗量子密码的研究方面, 还需要完善量子密码理论, 进一步研究量子密钥分配技术、量子身份认证技术和量子加密技术, 解决传输距离、传输速度、系统稳定性等多个问题, 同时量子密码的协议安全性分析也是研究的热点. 2) 面向云计算领域的高效加密技术: 在云计算应用领域, 全同态加密机制需要研究自然、简洁的构造方法, 从而提高加密机制的效率; 在可搜索加密机制方面需要完善理论和功能, 进一步研究支持模糊搜索、相关性排序和关系运算等问题, 改善用户体验; 在功能加密方面, 研究属性加密中密钥撤销、密钥滥用、策略隐藏和多授权等问题, 实现在云环境中的大范围应用. 3) 面向物联网应用的轻量级加密技术: 在物联网应用领域, 作为新兴的密码技术, 轻量级密码的理论分析还不够完善, 研究高效率、强鲁棒性的轻量级密码, 以及基于安全性和性能的轻量级密码评估方法, 将大大推动轻量级密码在物联网时代的发展.

4 结束语

网络空间安全不仅关系到人们的日常生活, 更是事关国家安全和国家发展的重大战略问题. 鉴于

网络空间面临着从物理层安全接入到数据层用户数据安全保护等各个层面的挑战, 迫切需要进行全面而系统化的安全基础理论和技术研究. 本文构建了涵盖物理层、系统层、网络层、数据层以及安全基础理论研究的 “四横一纵” 的层次化研究体系, 并对 6 个研究领域进行了重点阐述.

总体而言, 网络空间安全的发展趋势可以总结为传统领域面临新挑战、新计算模式诱发新问题、新网络形态导致新威胁、新基础理论促生新方法, 即 1) 随着工业 4.0 战略的提出, 工业化和信息化进一步融合, 推动了传统工业控制领域的转型升级, 但也暴露了其重视功能性实现、忽视安全性开发的痼疾, 需要设计覆盖供产销各个环节的整体安全防护方案; 2) 随着云计算、大数据等新型计算模式的发展, 通过数据分析可从庞大的网络数据中挖掘出大量的用户隐私信息, 给用户隐私保护带来了新的挑战, 需要研究新型访问控制和数据加密技术; 3) 物联网、移动互联网等多种新型网络形态的出现, 在驱动相关应用发展的同时, 潜在着更大的隐私泄露风险, 需要研究人 – 机 – 物相互认证和安全通信技术; 4) 量子计算理论的突破可以有效解决离散对数和因子分解问题, 彻底颠覆了传统密码学理论, 亟需研究新型的抗量子密码基础理论来应对挑战.

当然, 作为一个大的综合性研究学科, 网络空间安全研究覆盖面很广, 除了上述研究领域外, 还包括信息对抗、可信计算、数据灾备、数字取证等等众多未提及的方向, 这些研究方向也都有待于广大科研人员的进一步深入研究和探讨.

致谢 本文的撰写得到了熊润群博士和郭桃林、郭乃瑄、潘培龙、魏娜、李晓云、刘耀文、尹长昕、周佳欢等研究生的帮助, 以及江苏省网络与信息安全重点实验室 (BM2003201)、计算机网络和信息集成教育部重点实验室 (93K-9) 的资助. 特此表示感谢!

参考文献

1 Fang B X. A hierarchy model on the research fields of cyberspace security technology. Chinese J Netw Inf Secur, 2016, 1: 2–7 [方滨兴. 从层次角度看网络空间安全技术的覆盖领域. 网络与信息安全学报, 2016, 1: 2–7]
2 Li H, Zhang N. Suggestions on cyber security talents cultivation. Chinese J Netw Inf Secur, 2016, 1: 18–23 [李晖, 张宁. 网络空间安全学科人才培养之思考. 网络与信息安全学报, 2016, 1: 18–23]
3 Li J H, Qiu W D, Meng K, et al. Discipline construction and talents training of cyberspace security. J Inf Secur Res, 2015, 1: 149–154 [李建华, 邱卫东, 孟魁, 等. 网络空间安全一级学科内涵建设和人才培养思考. 信息安全研究, 2015, 1: 149–154]
4 Danev B, Zanetti D, Capkun S. On physical-layer identification of wireless devices. ACM Comput Surv, 2012, 45: 1–29
5 Tekbas Ö H, Serinken N, Üreten O. An experimental performance evaluation of a novel radio-transmitter identification system under diverse environmental conditions. Canadian J Electr Comput Eng, 2004, 29: 203–209
6 Rasmussen K B, Capkun S. Implications of radio fingerprinting on the security of sensor networks. In: Proceedings of the 3rd International Conference on Security and Privacy in Communications Networks and the Workshops, Nice, 2007. 331–340
7 Reising D R, Temple M A, Mendenhall M J. Improved wireless security for GMSK-based devices using RF fingerprinting. Int J Electron Secur Digit Foren, 2010, 3: 41–59
8 Brik V, Banerjee S, Gruteser M, et al. Wireless device identification with radiometric signatures. In: Proceedings of the 14th ACM international conference on Mobile computing and networking, San Francisco, 2008. 116–127
9 Gerdes R M, Daniels T E, Mina M, et al. Device identification via analog signal fingerprinting: a matched filter approach. In: Proceedings of the Network and Distributed System Security Symposium, San Diego, 2006. 1–11
10 Gerdes R M, Mina M, Russell S F, et al. Physical-layer identification of wired Ethernet devices. IEEE Trans Inf Foren Secur, 2012, 7: 1339–1353
11 Danev B, Heydt-Benjamin T S, Capkun S. Physical-layer identification of RFID devices. In: Proceedings of the 18th

Conference on USENIX Security Symposium, Montreal, 2009. 199–214
12 Dey S, Roy N, Xu W, et al. AccelPrint: imperfections of accelerometers make smartphones trackable. In: Proceedings of the Network and Distributed System Security Symposium, San Diego, 2014. 1–16
13 Das A, Borisov N, Caesar M. Do you hear what I hear? fingerprinting smart devices through embedded acoustic components. In: Proceedings of the ACM SIGSAC Conference on Computer and Communications Security, Arizona, 2014. 441–452
14 Zhou Z, Diao W, Liu X, et al. Acoustic fingerprinting revisited: Generate stable device id stealthily with inaudible sound. In: Proceedings of the ACM SIGSAC Conference on Computer and Communications Security, Arizona, 2014. 429–440
15 Maurer U M. Secret key agreement by public discussion from common information. IEEE Trans Inf Theory, 1993, 39: 733–742
16 Mathur S, Trappe W, Mandayam N, et al. Radio-telepathy: extracting a secret key from an unauthenticated wireless channel. In: Proceedings of the 14th ACM International Conference on Mobile Computing and Networking, San Francisco, 2008. 128–139
17 Jana S, Premnath S N, Clark M, et al. On the effectiveness of secret key extraction from wireless signal strength in real environments. In: Proceedings of the 15th ACM international Conference on Mobile Computing and Networking, Beijing, 2009. 321–332
18 Patwari N, Croft J, Jana S, et al. High-rate uncorrelated bit extraction for shared secret key generation from channel measurements. IEEE Trans Mobile Comput, 2010, 9: 17–30
19 Liu H, Yang J, Wang Y, et al. Collaborative secret key extraction leveraging received signal strength in mobile wireless networks. In: Proceedings of the 31st IEEE International Conference on Computer Communications, Orlando, 2012. 927–935
20 Yasukawa S, Iwai H, Sasaoka H. Adaptive key generation in secret key agreement scheme based on the channel characteristics in OFDM. In: Proceedings of International Symposium on Information Theory and its Applications, Auckland, 2008. 1–6
21 Sayeed A, Perrig A. Secure wireless communications: secret keys through multipath. In: Proceedings of IEEE International Conference on Acoustics, Speech and Signal Processing, Las Vegas, 2008. 3013–3016
22 Wang Q, Su H, Ren K, et al. Fast and scalable secret key generation exploiting channel phase randomness in wireless networks. In: Proceedings of the 30th IEEE International Conference on Computer Communications, Shanghai, 2011. 1422–1430
23 Liu Y, Draper S C, Sayeed A M. Exploiting channel diversity in secret key generation from multipath fading randomness. IEEE Trans Inf Foren Secur, 2012, 7: 1484–1497
24 Chou T H, Draper S C, Sayeed A M. Impact of channel sparsity and correlated eavesdropping on secret key generation from multipath channel randomness. In: Proceedings of IEEE International Symposium on Information Theory, Austin, 2010. 2518—2522
25 Studnia I, Alata E, Deswarte Y, et al. Survey of security problems in cloud computing virtual machines. In: Proceedings of Computer and Electronics Security Applications Rendez-vous, Rennes, 2012. 61–74
26 Ferrie P. Attacks on more virtual machine emulators. Symantec Advanced Threat Res, 2007. 1–17
27 Ristenpart T, Tromer E, Shacham H, et al. Hey, you, get off of my cloud: exploring information leakage in third-party compute clouds. In: Proceedings of the 16th ACM conference on Computer and communications security, Chicago, 2009. 199–212
28 King S T, Chen P M. SubVirt: implementing malware with virtual machines. In: Proceedings of IEEE Symposium on Security and Privacy, Oakland, 2006. 1–14
29 Nance K, Bishop M, Hay B. Virtual machine introspection: observation or interference? IEEE Secur Priv, 2008, 5: 32–37
30 Payne B D, Carbone M, Sharif M, et al. Lares: an architecture for secure active monitoring using virtualization. In: Proceedings of IEEE Symposium on Security and Privacy, Oakland, 2008. 233–247
31 Ibrahim A S, Hamlyn-Harris J, Grundy J, et al. CloudSec: a security monitoring appliance for Virtual Machines in the IaaS cloud model. In: Proceedings of the 5th International Conference on Network and System Security, Milan, 2011. 113–120

32 Yao F, Sprabery R, Campbell R H. CryptVMI: a flexible and encrypted virtual machine introspection system in the cloud. In: Proceedings of the 2nd international workshop on Security in cloud computing, Kyoto, 2014. 11–18

33 Seshadri A, Luk M, Qu N, et al. SecVisor: a tiny hypervisor to provide lifetime kernel code integrity for commodity OSes. In: Proceedings of the 21st ACM SIGOPS symposium on Operating systems principles, Washington, 2007. 335–350

34 Litty L, Lagar-Cavilla H A, Lie D. Hypervisor support for identifying covertly executing binaries. In: Proceedings of the 17th Conference on Security Symposium, Berkeley, 2008. 243–258

35 Wang Y D, Yang J H, Xu C, et al. Survey on access control technologies for cloud computing. J Soft, 2015, 26: 1129–1150 [王于丁, 杨家海, 徐聪, 等. 云计算访问控制技术研究综述. 软件学报, 2015, 26: 1129–1150]

36 Li X Y, Shi Y, Guo Y, et al. Multi-tenancy based access control in cloud. In: Proceedings of International Conference on Computational Intelligence and Software Engineering, Wuhan, 2010. 1–4

37 Tang B, Sandhu R, Li Q. Multi-tenancy authorization models for collaborative cloud services. Concurr Comput Pract Exper, 2015, 27: 2851–2868

38 Kurmus A, Gupta M, Pletka R, et al. A comparison of secure multi-tenancy architectures for filesystem storage clouds. In: Proceedings of the 12th International Middleware Conference, Laxenburg, 2011. 460–479

39 Popa L, Yu M, Ko S Y, et al. CloudPolice: taking access control out of the network. In: Proceedings of the 9th ACM SIGCOMM Workshop on Hot Topics in Networks, Monterey, 2010, 7. 1–6

40 Azab A M, Ning P, Wang Z, et al. HyperSentry: enabling stealthy in-context measurement of hypervisor integrity. In: Proceedings of the 17th ACM Conference on Computer and Communications Security, Chicago, 2010. 38–49

41 Wang Z, Jiang X. Hypersafe: a lightweight approach to provide lifetime hypervisor control-flow integrity. In: Proceedings of IEEE Symposium on Security and Privacy, Oakland, 2010. 380–395

42 Zhang F, Chen J, Chen H, et al. CloudVisor: retrofitting protection of virtual machines in multi-tenant cloud with nested virtualization. In: Proceedings of the 23rd ACM Symposium on Operating Systems Principles, Cascais, 2011. 203–216

43 Heiser G, Uhlig V, LeVasseur J. Are virtual-machine monitors microkernels done right? ACM SIGOPS Operating Syst Rev, 2006, 40: 95–99

44 Klein G, Elphinstone K, Heiser G, et al. seL4: formal verification of an OS kernel. In: Proceedings of the 22nd ACM SIGOPS Symposium on Operating Systems Principles, Big Sky, 2009. 207–220

45 Azab A M, Swidowski K, Bhutkar J M, et al. SKEE: a lightweight secure kernel-level execution environment for ARM. In: Proceedings of Network and Distributed System Security Symposium, San Diego, 2016. 1–15

46 Suh E, Ferraiuolo A, Wang Y, et al. Full-Processor Timing Channel Protection with Applications to Secure Hardware Compartments. Computing and Information Science Technical Reports, 2015. 1–15

47 Xia Y, Liu Y, Guan H, et al. Secure outsourcing of virtual appliance. IEEE Trans Cloud Comput, 2015, 99: 1–15

48 Ling Z, Luo J, Chen Q, et al. Secure fingertip mouse for mobile devices. In: Proceedings of the 35th Annual IEEE International Conference on Computer Communications, San Francisco, 2016. 1–9

49 Aviv A J, Gibson K, Mossop E, et al. Smudge attacks on smartphone touch screens. In: Proceedings of the 4th USENIX Workshop on Offensive Technologies, Washington, 2010. 1–10

50 Gao H, Ren Z, Chang X, et al. A new graphical password scheme resistant to shoulder-surfing. In: Proceedings of the International Conference on Cyberworlds, Singapore, 2010. 194–199

51 Kwon T, Na S. TinyLock: affordable defense against smudge attacks on smartphone pattern lock systems. Comput Secur, 2014, 42: 137–150

52 Bojinov H, Boneh D. Mobile token-based authentication on a budget. In: Proceedings of the 12th Workshop on Mobile Computing Systems and Applications, Phoenix, 2011. 14–19

53 Chen S, Pande A, Mohapatra P. Sensor-assisted facial recognition: an enhanced biometric authentication system for smartphones. In: Proceedings of the 12th International Conference on Mobile Systems, Applications, and Services, Bretton Woods, 2014. 109–122

54 Cheng K Y, Kumar A. Contactless finger knuckle identification using smartphones. In: Proceedings of the International Conference of the Biometrics Special Interest Group, Darmstadt, 2012. 1–6

55 Shabrina N, Akbar S, Ruswono P. Palmprint authentication in smartphone using phase-only correlation method. In: Proceedings of the 5th International Conference on Advanced Computer Science and Information Systems, Bali,

2013. 397–402
56 Raja K B, Raghavendra R, Stokkenes M, et al. Smartphone authentication system using periocular biometrics. In: Proceedings of the International Conference of the Biometrics Special Interest Group, Darmstadt, 2014. 1–8
57 de Luca A, Hang A, Brudy F, et al. Touch me once and I know it's you! implicit authentication based on touch screen patterns. In: Proceedings of the 30th ACM Conference on Human Factors in Computing Systems, Austin, 2012. 987–996
58 Clarke N L, Furnell S M. Authenticating mobile phone users using keystroke analysis. Int J Inf Secur, 2007, 6: 1–14
59 Giuffrida C, Majdanik K, Conti M, et al. I sensed it was you: authenticating mobile users with sensor-enhanced keystroke dynamics. In: Detection of Intrusions and Malware, and Vulnerability Assessment. Berlin: Springer, 2014. 92–111
60 Burgbacher U, Hinrichs K. An implicit author verification system for text messages based on gesture typing biometrics. In: Proceedings of the 32nd ACM Conference on Human Factors in Computing Systems, Toronto, 2014. 2951–2954
61 Derawi M O, Nickel C, Bours P, et al. Unobtrusive user-authentication on mobile phones using biometric gait recognition. In: Proceedings of the 6th International Conference on Intelligent Information Hiding and Multimedia Signal Processing, Darmstadt, 2010. 306–311
62 Feng T, Liu Z, Kwon K A, et al. Continuous mobile authentication using touchscreen gestures. In: Proceedings of the IEEE Conference on Technologies for Homeland Security, Waltham, 2012. 451–456
63 Frank M, Biedert R, Ma E D, et al. Touchalytics: on the applicability of touchscreen input as a behavioral biometric for continuous authentication. IEEE Trans Inf Foren Secur, 2013, 8: 136–148
64 Shen C, Zhang Y, Cai Z, et al. Touch-interaction behavior for continuous user authentication on smartphones. In: Proceedings of the 8th International Conference on Biometrics, Phuket, 2015. 157–162
65 Jakobsson M, Shi E, Golle P, et al. Implicit authentication for mobile devices. In: Proceedings of the 4th USENIX Workshop on Hot Topics in Security, Montreal, 2009. 9–14
66 Conti M, Zachia-Zlatea I, Crispo B. Mind how you answer me! In: Proceedings of the 6th ACM Symposium on Information, Computer and Communications Security, Hong Kong, 2011. 249–259
67 McLaughlin S, Podkuiko D, McDaniel P. Energy theft in the advanced metering infrastructure. Crit Inf Infrastructures Secur, 2009, 6027: 176–187
68 Varodayan D P, Gao G X. Redundant metering for integrity with information-theoretic confidentiality. In: Proceedings of the 1st IEEE International Conference on Smart Grid Communications, Gaithersburg, 2010. 345–349
69 Liu N, Chen J, Zhu L, et al. A key management scheme for secure communications of advanced metering infrastructure in smart grid. IEEE Trans Ind Electron, 2013, 60: 4746–4756
70 Diao F, Zhang F, Cheng X. A privacy-preserving smart metering scheme using linkable anonymous credential. IEEE Trans Ind Electron, 2015, 6: 461–467
71 Li F, Luo B, Liu P. Secure information aggregation for smart grids using homomorphic encryption. In: Proceedings of the 1st IEEE International Conference on Smart Grid Communications, Gaithersburg, 2010. 327–332
72 Li H, Mao R, Lai L, et al. Compressed meter reading for delay-sensitive and secure load report in smart grid. In: Proceedings of the 1st IEEE International Conference on Smart Grid Communications, Gaithersburg, 2010. 114–119
73 Rial A, Danezis G. Privacy-preserving smart metering. In: Proceedings of the 10th Annual ACM Workshop on Privacy in the Electronic Society, Chicago, 2011. 49–60
74 Ruj S, Nayak A. A decentralized security framework for data aggregation and access control in smart grids. IEEE Trans Ind Electron, 2013, 4: 196–205
75 Rottondi C, Verticale G, Capone A. Privacy-preserving smart metering with multiple data consumers. Comput Netw, 2013, 57: 1699–1713
76 Birman K, Jelasity M, Kleinberg R, et al. Building a secure and privacy-preserving smart grid. ACM Special Interest Group Operating Syst Rev, 2015, 49: 131–136
77 Yuan Y, Li Z, Ren K. Modeling load redistribution attacks in power systems. IEEE Trans Smart Grid, 2011, 2: 382–390
78 Liu Y, Ning P, Reiter M K. False data injection attacks against state estimation in electric power grids. ACM Trans Inf Syst Secur, 2011, 14: 1–33
79 Huang Y, Esmalifalak M, Nguyen H, et al. Bad data injection in smart grid: attack and defense mechanisms. IEEE

Commun Mag, 2013, 51: 27–33
80 Yu Z H, Chin W L. Blind false data injection attack using pca approximation method in smart grid. IEEE Trans Smart Grid, 2015, 6: 1219–1226
81 Bobba R B, Rogers K M, Wang Q, et al. Detecting false data injection attacks on dc state estimation. In: Proceedings of the 1st Workshop on Secure Control Systems, Stockholm, 2010. 1–9
82 Dán G, Sandberg H. Stealth attacks and protection schemes for state estimators in power systems. In: Proceedings of the 1st IEEE International Conference on Smart Grid Communications, Gaithersburg, 2010. 214–219
83 Liu L, Esmalifalak M, Ding Q, et al. Detecting false data injection attacks on power grid by sparse optimization. IEEE Trans Smart Grid, 2014, 5: 612–621
84 Lu Z, Lu X, Wang W, et al. Review and evaluation of security threats on the communication networks in the smart grid. In: Proceedings of IEEE Military Communications Conference, San Jose, 2010. 1830–1835
85 Li H, Lai L, Qiu R C. Communication capacity requirement for reliable and secure state estimation in smart grid. In: Proceedings of the 1st IEEE International Conference on Smart Grid Communications, Gaithersburg, 2010. 191–196
86 Khurana H, Bobba R, Yardley T, et al. Design principles for power grid cyber-infrastructure authentication protocols. In: Proceedings of the 43rd Hawaii International Conference on System Sciences, Hawaii, 2010. 1–10
87 Yang M, Luo J, Ling Z, et al. De-anonymizing and countermeasures in anonymous communication networks. IEEE Commun Mag, 2015, 53: 60–66
88 Edman M, Syverson P. AS-awareness in tor path selection. In: Proceedings of the 16th ACM Conference on Computer and Communications Security, Chicago, 2009. 380–389
89 Murdoch S J, Zieliński P. Sampled traffic analysis by internet-exchange-level adversaries. In: Proceedings of the Privacy Enhancing Technologies, Berlin, 2007. 167–183
90 Johnson A, Wacek C, Jansen R, et al. Users get routed: traffic correlation on tor by realistic adversaries. In: Proceedings of the 20th ACM Conference on Computer and Communications Security, Berlin, 2013. 337–348
91 Bauer K, McCoy D, Grunwald D, et al. Low-resource routing attacks against Tor. In: Proceedings of the ACM Workshop on Privacy in the Electronic Society, Alexandria, 2007. 11–20
92 Pappas V, Athanasopoulos E, Ioannidis S, et al. Compromising anonymity using packet spinning. In: Proceedings of the 11th Information Security Conference, Taipei, 2008. 161–174
93 Yu W, Fu X, Graham S, et al. DSSS-based flow marking technique for invisible traceback. In: Proceedings of IEEE Symposium on Security and Privacy, Oakland, 2007. 18–32
94 Houmansadr A, Kiyavash N, Borisov N. RAINBOW: a robust and invisible non-blind watermark for network flows. In: Proceedings of the 16th Annual Network & Distributed System Security Symposium, San Diego, 2009. 1–13
95 Wang X, Luo J, Yang M. An interval centroid based spread spectrum watermark for tracing multiple network flows. In: Proceedings of IEEE International Conference on Systems, Man, and Cybernetics, San Antonio, 2009. 4000–4006
96 Ling Z, Luo J, Yu W, et al. A new cell counter based attack against tor. In: Proceedings of the 16th ACM Conference on Computer and Communications Security, Chicago, 2009. 578–589
97 Ling Z, Luo J, Yu W, et al. Protocol-level attacks against tor. Comput Netw, 2013, 57: 869–886
98 Ling Z, Fu X, Jia W, et al. Novel packet size-based covert channel attacks against anonymizer. IEEE Trans Comput, 2013, 62: 2411–2426
99 Wang X, Luo J, Yang M, et al. A potential HTTP-based application-level attack against tor. Future Gener Comput Syst, 2011, 27: 67–77
100 Chakravarty S, Barbera M V, Portokalidis G, et al. On the effectiveness of traffic analysis against anonymity networks using flow records. In: Proceedings of Passive and Active Measurement Conference, Los Angeles, 2014. 247–257
101 Hintz A. Fingerprinting websites using traffic analysis. In: Proceedings of the 2nd International Conference on Privacy Enhancing Technologies, San Francisco, 2002. 171–178
102 Liberatore M, Levine B N. Inferring the source of encrypted HTTP connections. In: Proceedings of the 13th ACM Conference on Computer and Communications Security, Alexandria, 2006. 255–263
103 Panchenko A, Niessen L, Zinnen A, et al. Website fingerprinting in onion routing based anonymization networks. In: Proceedings of the 10th Annual ACM Workshop on Privacy in the Electronic Society, New York, 2011. 103–114
104 Cai X, Zhang X C, Joshi B, et al. Touching from a distance: website fingerprinting attacks and defenses. In: Proceedings of the ACM Conference on Computer and Communications Security, New York, 2012. 605–616

105 Wang T, Cai X, Nithyanand R, et al. Effective attacks and provable defenses for website fingerprinting. In: Proceedings of the 23rd USENIX Security Symposium, San Diego, 2014. 143–157
106 He G, Yang M, Gu X, et al. A novel active website fingerprinting attack against tor anonymous system. In: Proceedings of the 18th IEEE International Conference on Computer Supported Cooperative Work in Design, Hsinchu, 2014. 112–117
107 Bennett C H, Brassard G. Quantum cryptography: public key distribution and coin tossing. In: Proceedings of IEEE International Conference on Computer System and Signal Processing, New York, 1984. 175–179
108 Lo H K, Chau H F. Unconditional security of quantum key distribution over arbitrarily long distances. Science, 1999, 283: 2050–2056
109 Ekert A K. Quantum cryptography based on Bell's theorem. Phys Rev Lett, 1991, 67: 661–663
110 Bennett C H. Quantum cryptography using any two nonorthogonal states. Phys Rev Lett, 1992, 68: 3121–3124
111 Peng C Z, Yang T, Bao X H, et al. Experimental free-space distribution of entangled photon pairs over 13 km: towards satellite-based global quantum communication. Phys Rev Lett, 2005, 94: 1–4
112 Peng C Z, Zhang J, Yang D, et al. Experimental long-distance decoy-state quantum key distribution based on polarization encoding. Phys Rev Lett, 2007, 98: 1–4
113 Jin X M, Ren J G. Experimental free-space quantum teleportation. Nature Photon, 2010, 4: 376–381
114 Hoffstein J, Pipher J, Silverman J H. NTRU: a ring-based public key cryptosystem. In: Proceedings of the 3rd International Symposium on Algorithmic Number Theory, Portland, 1998. 267–288
115 Regev O. On lattices, learning with errors, random linear codes, and cryptography. J ACM, 2009, 56: 34–73
116 Gentry C. Fully homomorphic encryption using ideal lattices. In: Proceedings of the 41st ACM Symposium on Theory of Computing, Bethesda, 2009. 169–178
117 Agrawal S, Boneh D, Boyen X. Efficient lattice (H) IBE in the standard model. In: Proceedings of the 29th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Riviera, 2010. 553–572
118 Lyubashevsky V. Lattice signatures without trapdoors. In: Proceedings of the 31st Annual International Conference on the Theory and Applications of Cryptographic Techniques, Cambridge, 2012. 738–755
119 Adleman L M. Molecular computation of solutions to combinatorial problems. Science, 1994, 266: 1021–1024
120 Tang J, Cui Y, Li Q, et al. Ensuring security and privacy preservation for cloud data services. ACM Comput Surv, 2016, 49: 1–39
121 Rivest R L, Adleman L, Dertouzos M L. On data banks and privacy homomorphisms. Found Secure Comput, 1978, 4: 169–180
122 van Dijk M, Gentry C, Halevi S, et al. Fully homomorphic encryption over the integers. In: Proceedings of the 29th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Riviera, 2010. 24–43
123 Song D X, Wagner D, Perrig A. Practical techniques for searches on encrypted data. In: Proceedings of IEEE Symposium on Security and Privacy, Berkeley, 2000. 44–55
124 Boneh D, Di Crescenzo G, Ostrovsky R, et al. Public key encryption with keyword search. In: Proceedings of International Conference on the Theory and Applications of Cryptographic Techniques, Interlaken, 2004. 506–522
125 Cao N, Wang C, Li M, et al. Privacy-preserving multi-keyword ranked search over encrypted cloud data. IEEE Trans Parall Distrib Syst, 2014, 25: 222–233
126 Sahai A, Waters B. Fuzzy identity-based encryption. In: Proceedings of the 24th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Aarhus, 2005. 457–473
127 Lewko A, Okamoto T, Sahai A, et al. Fully secure functional encryption: attribute-based encryption and (hierarchical) inner product encryption. In: Proceedings of the 29th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Riviera, 2010. 62–91
128 O'Neill A. Definitional issues in functional encryption. IACR Cryptology ePrint Archive, 2010. 1–11
129 Boneh D, Sahai A, Waters B. Functional encryption: definitions and challenges. Theory Cryptogr, 2011, 6597: 253–273
130 Naveed M, Agrawal S, Prabhakaran M, et al. Controlled functional encryption. In: Proceedings of the ACM SIGSAC Conference on Computer and Communications Security, Arizona, 2014. 1280–1291
131 David M, Ranasinghe D C, Larsen T. A2U2: a stream cipher for printed electronics RFID tags. In: Proceedings of IEEE International Conference on RFID, Orlando, 2011. 176–183

132 Saarinen M J O. The BlueJay ultra-lightweight hybrid cryptosystem. In: Proceedings of IEEE Symposium on Security and Privacy Workshops, San Francisco, 2012. 27–32
133 Gong Z. Survey on lightweight hash functions. J Cryptologic Res, 2016, 3: 1–11 [龚征. 轻量级 Hash 函数研究. 密码学报, 2016, 3: 1–11]
134 Bogdanov A, Knežević M, Leander G, et al. SPONGENT: a lightweight hash function. In: Proceedings of the 13th International Workshop on Cryptographic Hardware and Embedded Systems, Nara, 2011. 312–325
135 Yoshida H, Watanabe D, Okeya K, et al. MAME: a compression function with reduced hardware requirements. In: Proceedings of the 9th International Workshop on Cryptographic Hardware and Embedded Systems, Vienna, 2007. 148–165
136 Hirose S, Ideguchi K, Kuwakado H, et al. A lightweight 256-bit hash function for hardware and low-end devices: lesamnta-LW. In: Proceedings of the 13th International Conference on Information Security and Cryptology, Seoul, 2010. 151–168
137 Kuwakado H, Hirose S. Hashing mode using a lightweight blockcipher. In: Proceedings of the 14th IMA International Conference on Cryptography and Coding, Oxford, 2013. 213–231
138 Billet O, Robshaw M J B, Peyrin T. On building hash functions from multivariate quadratic equations. In: Proceedings of the 12th Australasian Conference Information Security and Privacy, Townsville, 2007. 82–95
139 Bettale L, Faugere J C, Perret L. Security analysis of multivariate polynomials for hashing. In: Proceedings of the 11th International Conference Information Security and Cryptology, Seoul, 2008. 115–124

Architecture and key technologies of cyberspace security

Junzhou LUO*, Ming YANG, Zhen LING, Wenjia WU & Xiaodan GU

School of Computer Science and Engineering, Southeast University, Nanjing 211189*, China*
*E-mail: jluo@seu.edu.cn

Abstract Cyberspace is a dynamic virtual space composed of various critical information infrastructure components including Internet, communication networks, cyber-physical systems, and industrial control networks. It also includes incorporates interaction among humans, machines, and things. Cyberspace security involves both the security of the information infrastructure and the security of various data that are generated, processed, transmitted, and stored. With the rapid development of new technologies, such as cloud computing, big data, cyber-physical systems, and quantum computing, cyberspace security is being confronted with a series of new threats and challenges. To this end, in this paper, a cyberspace security research framework comprising four horizontal layers and one vertical layer is first established, including physical security, system security, network security, data security, and the basics of the security theory applied in each layer. On this basis, several basic theories and key technologies for priority development are investigated. The associated research fields are fingerprinting- and channel characteristics-based device authentication and secure communication, virtualization security analysis and defense in cloud computing environments, user authentication technology on mobile smart devices, security technology for electric power industry control systems in network environments, anonymous communication and traffic analysis technology, and basic theory for modern cryptography and data security mechanism. Development trends in the research on future cyberspace security are also explored.

Keywords cyberspace security, device fingerprint, virtualization security, continuous authentication, industry control system security, anonymous communication, cryptosystem

Junzhou LUO was born in 1960. He received a Ph.D. degree in computer networks from Southeast University, Nanjing, in 2000. Currently, he is a full professor at the School of Computer Science and Engineering in Southeast University, Nanjing, China. His research interests include next-generation networks, protocol engineering, network security, cloud computing, and wireless LAN. Professor Luo is a member of IEEE and ACM, as well as co-chair of the IEEE SMC Technical Committee on Computer Supported Cooperative Work in Design, and chair of ACM SIGCOMM China.

Zhen LING was born in 1982. He received a Ph.D. degree in computer science from Southeast University, China. Currently, he is an assistant professor at the School of Computer Science and Engineering in Southeast University, Nanjing, China. His research interests include smartphone security, network security, privacy, and forensics. Dr. Ling is a member of IEEE, ACM, and CCF.

Ming YANG was born in 1979. He received a Ph.D. degree in computer science from Southeast University, Nanjing, in 2007. Currently, he is an associate professor at the School of Computer Science and Engineering in Southeast University, Nanjing, China. His research interests include network security and privacy. Dr. Yang is a member of CCF and ACM, as well as deputy director of Key Laboratory of Computer Network and Information Integration, Ministry of Education.

Wenjia WU was born in 1983. He received a Ph.D. degree in computer science from Southeast University, Nanjing, in 2013. Currently, he is a lecturer at the School of Computer Science and Engineering in Southeast University. His research interests include computer networks. Dr. Wu is a member of CCF and ACM.