第十一届中国可信计算与信息安全学术会议

The 11th National Conference on Trusted Computing & Information Security

CTCIS 2017 程序册

湖南长沙　　2017.09

CTCIS 2017 组织机构

主办单位： 中国计算机学会

指导单位： 密码研究协同创新中心

教育部高等学校信息安全专业教学指导委员会

湖南省委网络安全和信息化领导小组办公室

承办单位： 国防科技大学

湖南大学

中国计算机学会容错计算专业委员会

协办单位： 武汉大学

湖南省信息网络安全协会

赞助单位： 蓝盾信息安全技术股份有限公司

可信计算组大中华地区论坛

清华大学出版社

合天智汇信息技术有限公司

大会名誉主席：沈昌祥，中国工程院院士

大会主席：王怀民，国防科技大学教授

大会副主席：张焕国，武汉大学教授

大会主席助理：赵　波，武汉大学教授

程序委员会共同主席：徐　明，国防科技大学教授

秦　拯，湖南大学教授

程序委员会副主席：严　飞，武汉大学副教授

组织委员会主席：王勇军，国防科技大学研究员

副主席：付绍静，国防科技大学副教授

指导委员会

主　任：沈昌祥　　北京工业大学

副主任：张焕国　　武汉大学

委　员：（按姓氏拼音排序）

陈　钟　　北京大学

陈克非　　杭州师范大学

冯登国　　北京信息科学技术研究院

韩　臻　　北京交通大学

贺也平　　中国科学院软件研究所

李建华　　上海交通大学

李舟军　　北京航空大学

马建峰　　西安电子科技大学

孟　丹　　中科院信息工程研究所

秦志光　　电子科技大学

宋书民　　密码研究协同创新中心

苏金树　　国防科技大学

王小云　　清华大学

王志英　　国防科技大学

谢晓尧　　贵州师范大学

杨晓元　　武警工程大学

杨义先　　北京邮电大学

朱智强　　信息工程大学

程序委员会委员

（按姓氏拼音排序）

常祖领	郑州大学
陈　飞	深圳大学
陈嘉耕	华中师范大学
陈　晶	武汉大学
陈　恺	中国科学院信息工程研究所
陈荣茂	国防科技大学
程庆丰	信息工程大学
丁　勇	桂林电子科技大学
杜瑞忠	河北大学
冯秀涛	中科院系统科学研究所
付　伟	海军工程大学
付章杰	南京信息工程大学
傅建明	武汉大学
郭山清	山东大学
郭渊博	信息工程大学
韩伟力	复旦大学
何德彪	武汉大学
胡玉鹏	湖南大学
黄　强	国家信息安全保障实验室
黄　琼	华南农业大学
黄欣沂	福建师范大学
贾春福	南开大学
姜文君	湖南大学
蒋伟进	湖南商学院

李发根　　成都电子科技大学
李洪伟　　成都电子科技大学
李　琦　　清华大学深圳研究生院
李长云　　湖南工业大学
林璟锵　　中国科学院信息工程研究所
刘　波　　国防科技大学
刘　烃　　西安交通大学
吕　品　　广西大学
屈龙江　　国防科技大学
邵　俊　　浙江工商大学
石文昌　　人民大学
宋　富　　华东师范大学
唐　明　　武汉大学
滕少华　　广东工业大学
田东海　　北京理工大学
田有亮　　贵州大学
王化群　　南京邮电大学
王劲松　　天津理工大学
王　伟　　北京交通大学
王伟平　　中南大学
王文贤　　四川大学
王勇军　　国防科技大学
魏悦川　　武警工程大学
伍前红　　北京航天航空大学
夏卓群　　长沙理工大学
鲜　明　　国防科技大学
肖　亮　　厦门大学

肖　伟　　湖南师范大学

谢　鲲　　湖南大学

徐明迪　　中船重工集团第 709 研究所

徐　鹏　　华中科技大学

许　力　　福建师范大学

姚孝明　　海南大学

赵　磊　　武汉大学

郑群雄　　信息工程大学

周芳芳　　中南大学

周学广　　海军工程大学

朱　辉　　西安电子科技大学

邹德清　　华中科技大学

会议议程一览表

日期	时间	内　　容			地点
9 月 14 日	14:30-21:00	参会代表报到、注册			长沙现代凯莱酒店大厅
	17:30-19:00	晚餐（自助餐）			一楼餐厅
	19:30-21:00	程序委员会扩大会议			第六会议室
9 月 15 日	7:00-8:30	早餐（自助）			一楼餐厅
	8:30-8:50	开幕式	徐明教授主持	领导与嘉宾致辞	现代厅
	8:50-9:10	合　　影			酒店门口
	9:10-9:50	特邀报告一	张焕国教授主持	题　目：Techniques for End-to-End Security in Mobile Computing 报告人：邓慧杰（新加坡管理大学信息安全首席教授，IEEE Fellow）	现代厅
	9:50-10:30	特邀报告二		题　目：Security & Privacy Assurance in Cloud Storage & Crowdsourcing Systems 报告人：贾小华（香港城市大学计算机系首席教授，IEEE Fellow）	现代厅
	10:30-10:50	茶　　歇			二楼廊区
	10:50-11:30	特邀报告三	徐明教授主持	题　目：新安全中的几个重要问题及其应对思路 报告人：杜跃进（阿里巴巴集团安全部副总裁）	现代厅
	11:30-12:10	特邀报告四		题　目：飞腾 CPU 实践与体会 报告人：窦强（国防科技大学教授）	
	12:10-13:30	自 助 午 餐			一楼餐厅
	13:30-18:00	分论坛		信息系统安全	第三会议室
				网络安全	第六会议室
				密码学	第八会议室
				内容安全与应用安全	第九会议室
	18:20-20:00	欢 迎 晚 餐			二楼宴会厅

日期	时间	内　　容			地点
9 月 16 日	7:00-8:30	早餐（自助）			一楼餐厅
	8:30-9:10	特邀报告五	杜瑞颖教授主持	题　目：区块链-理论与应用 报告人：张方国（中山大学教授）	岳麓厅
	9:10-10:20	自主与可控信息技术专题	许力教授主持	题　目：麒麟操作系统的实践与思考 报告人：戴华东 (国防科技大学)	
				题　目：以新思路应对网络空间安全挑战 报告人：王宝生（国防科技大学)	
				题　目：云数据库技术对可信计算的支持 报告人：孙家彦（优炫软件）	
	10:20-10:40	茶　　歇			
	10:40-11:50	互联网安全威胁与防范专题	秦拯教授主持	题　目：未知的博弈--威胁向量分析与防御 报告人：魏强（信息工程大学）	
				题　目：勒索病毒攻防漫谈 报告人：张悦（暨南大学）	
				题　目：“弱”密码的阴影-猜测密码攻击的一些进展 报告人：肖晟（湖南大学）	
	11:50-12:05	企业报告专题	王勇军研究员主持	题　目：云虚拟化安全 报告人：唐宏斌（蓝盾股份）	岳麓厅
	12:05-12:20			题　目：国际可信计算的愿景和创新战略 报告人：刘冬梅（微软可信赖计算部）	岳麓厅
	12:20-13:30	午餐（自助餐）			一楼餐厅
	13:30-18:00	分论坛		信息系统安全	第三会议室
				网络安全	第六会议室
				密码学	第八会议室
				内容安全与应用安全	第九会议室
	18:20-19:30	自助晚餐			一楼餐厅
9 月 17 日	7:00-8:30	早餐（自助）			一楼餐厅
	8:30-12:00	参观国家超算长沙中心和湖南湘江新区规划档案中心			酒店门口乘车

分组论坛安排

Session1：信息系统安全　时间：9月15日下午　地点：第三会议室

时间	主持人	报告人	单　位	题　　目
13:30-16:00	贾春福	高元照	解放军信息工程大学	A Cloud Computing Forensic Model
		郭　曦	华中农业大学	程序状态合并中隐式关联逆向分析方法
		王　亮	西安电子科技大学	A Signature-Sharing Based Auditing Scheme with Data Deduplication in Cloud Storage
		车　奔	四川大学	IaaS 环境中支持自定义算法的 VPNaaS 框架
		刘鹤群	西安电子科技大学	Public auditing for shared data utilizing backups with user revocation in the cloud
		刘峰宇	国防科技大学	基于文件签名认证的 DLL 加载漏洞防御技术研究
		姜百合	武汉大学	基于 Fuzzing 技术的云数据泄露漏洞检测研究
		尹学渊	四川大学	Research of Security as a Service for VMs in IaaS Platform
		徐　洋	贵州师范大学	一种 SDN 中 DDoS 检测及防御方法
		赵　波	武汉大学	Powermitter: Data Exfiltration from Air-Gapped Computer through Switching Power Supply
		王　勇	北京理工大学	An Approach of Implementing Core Role Based Access Control Model Using Attribute based Encryption
16:00-16:20	会议休息（茶歇）			
16:20-18:00	傅建明	乔延臣	深信服科技股份有限公司	A Cloud Security System Based on Security Resource
		陈晓帆	深信服科技股份有限公司	A Cloud Security Scheme Based on SDN
		徐明迪	武汉数学工程研究所	满足对应性属性的平台配置证明研究
		徐明迪	武汉数学工程研究所	Real-time Trusted Computing Technology for Xenomai System
		李志刚	北京工业大学	面向 Windows 移动环境进程主动动态度量方法研究
		蔡梦娟	四川大学	基于 KVM 的虚拟机进程代码分页式度量方法
		王小艳	四川大学	基于 OpenStack 的云计算网络性能测量与分析
		刘　飚	北京电子科技学院	A Research of Power Analysis Based on Ensemble Model
		秦煜瑶	北京航空航天大学	A New FPGA PUF Based on Transition Probability Delay Measurement
		石　原	武汉大学	CHAOS: an SDN-based Moving Target Defense System

Session2：密码学　时间：9月15日下午　地点：第八会议室

时间	主持人	报告人	单　位	题　　目
13:30-16:00	魏立斐	魏立斐	上海海洋大学	一种遥感图像的安全外包去噪方案
		刘成基	陕西师范大学	Quantum-secret-sharing scheme based on local distinguishability of orthogonal six-qudit entangled states
		刘娅茹	武警工程大学	安全多方计算中空间位置关系的保密判定
		罗小双	武警工程大学	基于双服务器模型的可公开验证多元多项式外包计算方案
		施泰荣	信息工程大学	Collision attacks against AEZ-prf for authenticated encryption AEZ
		邵栋阳	天津工业大学	两个电子货币方案的分析与改进
		白　平	武警工程大学	基于谓词的Paillier型密文解密外包方案
		张　青	黄冈师范学院	一种可证安全的代理聚合签名方案
		唐　明	武汉大学	A Generic TC--Based Method to Find the Weakness in Different Phases of Masking Schemes
16:00-16:20	会议休息（茶歇）			
	李雄	杨　超	信息工程大学	面向广域环境的量子密钥网络模型研究
		程　璐	武警工程大学	Midori算法的多维零相关线性分析
		李谢华	湖南大学	Decentralized Attribute-Based Encryption and Data Sharing Scheme in Cloud Storage
		高梓渊	西安电子科技大学	Verifiable Auditing Protocol with Proxy Re-encryption for Outsourced Databases in Cloud
		王亚辉	武汉大学	New Quantum Polynomial-time Fixed-point Attack for RSA based on Phase Estimation
		王亚辉	武汉大学	Analysis of RSA Quantum Algorithm not based on Factorization
		罗一帆	北京交通大学	一种基于组合公钥的密钥派生方案
		郭青霄	北京交通大学	基于SM2的代理保护代理签名的设计与实现

Session3：网络安全　时间：9月15日下午　地点：第六会议室

时间	主持人	报告人	单　位	题　　目
13:30-16:00	田俊锋	刘　政	辽宁工业大学	Design of Anti-eavesdropping Code Based on Fountain Codes
		赵陈佳昕	四川大学	基于虚拟机IO序列与Markov模型的异常行为检测研究
		朱　毅	四川大学	基于模糊综合评价模型的DNS健康度评估
		王丽艳	北京理工大学	Worms homology analysis method based on attack and propagation features
		孟　博	中南民族大学	安全协议实施安全性分析综述
		李　阳	武汉数字工程研究所	基于流量统计特征的网络潜在威胁用户挖掘方法研究
		杨　超	信息工程大学	Quantum key distribution Network: Optimal Secret-Key-Aware Routing Method for Trust Relaying
		张兴隆	信息工程大学	TLS 1.3协议研究进展
		张伟丽	东北大学	基于安全博弈的SDN数据包抽检策略
		刘利钊	厦门理工学院	基于量子辐射场的大数据安全存储寻址算法
		曹　咪	北京交通大学	TVOS应用分析与恶意应用检测方法研究
16:00-16:20	会议休息（茶歇）			
16:20-18:00	陈锦富	周伟伟	解放军信息工程大学	Detection and Suppression Algorithm against Narrowband-interference Attack in Wireless Sensor Networks Based on the Regret Matching
		陈敬涵	四川大学	基于TDRI的多视图关联DNS流量可视分析
		段洋洋	湖北民族学院	车联网中基于群签名的身份认证协议研究
		朱　丹	贵州师范大学	基于云模型与贝叶斯反馈的网络安全等级评估方法
		徐　慧	湖北工业大学	融合杜鹃搜索的灰狼优化算法在网络入侵检测特征选择中的应用
		叶晓鸣	四川大学	Research on the Anomaly Host Community Detection Model Based on Graph-Evolution Events
		叶晓鸣	四川大学	Efficient Feature Extraction Using Apache Spark for Network Behaviors Anomaly Detection
		韩珍辉	四川大学	面向高校校园网的OTM问题检测

Session4：内容安全与应用安全　时间：9 月 15 日下午　地点：第九会议室

时间	主持人	报告人	单　位	题　　目
13:30-16:00	康海燕	刘亚州	武警工程大学	基于博弈论的谣言传播研究
		KONATE AROUNA	武汉大学	Sentiment Analysis of Code-Mixed Bambara-French Social Media Text Using Deep Learning Techniques
		秦婉亭	石家庄铁道大学	Modeling and Analysis of Information Propagation Model of Online/Offline Network Based on Coupled Network
		康海燕	北京信息科技大学	基于视频分析的地理信息隐私保护方法研究
		康海燕	北京信息科技大学	基于身份替代的隐私保护方法研究
		张德阳	武警工程大学	基于用户相对影响权重的热点事件传播阈值模型
		张苗苗	北京邮电大学	Link privacy protection in Social Network based on neighborhood randomization algorithm
		高培贤	武警工程大学	基于卷积神经网络的图像隐写分析方法
		吕含笑	湖北民族学院	相同疾病数据集的隐私保护泛化算法研究
		熊　璐	武汉大学	一种新的基于 APP 启动模式的劫持攻击方案
16:00-16:20	会议休息（茶歇）			
16:20-18:00	严　飞	付　伟	武警工程大学	Bass-SI 社交网络谣言传播模型研究
		李天雪	武警工程大学	基于同态公钥加密系统的可逆信息隐藏算法
		狄富强	武警工程大学	Double-layered predictor for high-fidelity reversible data hiding
		马晨曦	四川大学	基于改进的 CCLDA 多数据源热点话题检测模型
		孙　岚	福州大学	A Consistency Optimization Algorithm for Differential Privacy Streaming Data Publication with Non-uniform Private Budget
		王建平	武警工程大学	基于码分多址复用的密文域可逆信息隐藏算法
		李　栋	武警工程大学	基于残差三维直方图调整的 H.264 可逆信息隐藏
		伊华伟	辽宁工业大学	Robust recommendation algorithm based on kernel principal component analysis and fuzzy c-means clustering

Session5：信息系统安全　时间：9月16日下午　地点：第三会议室

时间	主持人	报告人	单　位	题　　目
13:30-16:00	彭国军	单　纯	北京理工大学	Software system evolution method based on algebraic topology
		张欣欣	福建师范大学	平衡超立方体的故障容错性
		王丽娜	武汉大学	面向云平台的硬件辅助 ROP 检测方法
		胡岸琪	武汉大学	一种基于多层监测的 Struts2 未知漏洞攻击检测与细节回溯方案
		魏国珩	海军工程大学	A lightweight RFID authentication protocol scheme based on ECC
		龙　宇	上海交通大学	具有高表达能力的新型可信计算信任链的设计
		齐　能	四川师范大学	一种具有瀑布特征的可信虚拟平台信任链模型
		何欣枫	河北大学	A Trusted VM Live Migration Protocol in IaaS
		王小峰	国防科技大学	T-IP: A Self-Trustworthy and Secure Internet Protocol
		蒋伟进	湘潭大学	A Trusted Service Selection Method Based on User's Personality Feature and Service Recommendation
		孙家泽	西安邮电大学	The Software Module Clustering Algorithm Using Probability Selection
		田俊峰	河北大学	Classification of video-based public opinion via projection metric learning with Riemannian triplet constraint
16:00-16:20	会议休息（茶歇）			
16:20-18:00	杜瑞忠	杜瑞忠	河北大学	Dynamic Integrity Measurement Model Based on vTPM
		黄坚会	北京工业大学	TPCM 三阶三路安全可信架构
		公　备	北京工业大学	A Trusted Attestation Mechanism for the Sensing Nodes of Internet of Things Based on Dynamic Trusted Measurement
		肖源源	贵州大学	The Security Authentication of Biometrics Recognition Based On RGB-D
		康海燕	北京信息科技大学	面向用户的电商平台刷单行为智能检测方法研究
		夏卓群	长沙理工大学	一种基于路径分析的电力 CPS 攻击预测方法
		金俊杰	南京邮电大学	Enhancing Android Permission Management through Simulation Data Configuration
		李　津	北京系统工程研究所	An Integration Testing Framework for Software Vulnerability Detection Method

Session6：密码学　时间：9月16日下午　地点：第八会议室

时间	主持人	报告人	单　位	题　　目
13:30-16:00	陈荣茂	李陶深	广西大学	云环境中基于代理重加密的多用户全同态加密方案
		李大伟	北京航空航天大学	Revocable Hierarchical Identity-Based Broadcast Encryption
		张　凯	信息工程大学	Automatic Search of Impossible Differentials and Zero-Correlation Linear Hulls for ARX Ciphers
		韩海清	武汉大学	Algorithms research of McEliece and Niederreiter public-key cryptosystem based on quantum BCH codes
		屈　娟	重庆三峡学院	Cryptanalysis and security enhancement of an efficient secure authentication scheme with user anonymity for roaming user in ubiquitous networks
		黄晓芳	西南科技大学	基于区块链的云计算电子取证系统开发
		崔竞一	信息工程大学	Improved Impossible Differential Attacks on Large-Block Rijndael
		玄鹏开	东北大学	支持多用户操作的外包数据库可验证方案
16:00-16:20	会议休息（茶歇）			
	付绍静	吴福生	武汉大学	A Dictionary Sequence Model to Analyze the Security of Protocol Implementations at the Source Code Level
		李新超	武警工程大学	基于秘密共享的SMS4算法S盒的设计与优化
		吴旭光	武警工程大学	Parallel Long Messages Encryption Algorithm based on Certificateless Cryptosystem
		贾建卫	武汉大学	Cryptanalysis of a cryptosystem with noncommutative platform groups
		章红艳	福建师范大学协和学院	传感器网络中基于超立方体的对密钥建立方案
		马双棚	武警工程大学	一种适用于SMS4的改进RSM掩码方案

Session7：网络安全　时间：9月16日下午　地点：第六会议室

时间	主持人	报告人	单　位	题　　目
13:30-16:00	王　志	王　志	南开大学	A Learning Evasive Email-based P2P-like Botnet
		欧　露	湖南大学	An Efficient and Privacy-preserving Multi-user Cloud-based LBS Query Scheme
		谭　韧	空军工程大学	A Software Defined APT Attack Moving Target Defense Network Architecture
		杨　爽	东北大学	移动社交网络中基于信任评估机制的安全路由机制
		程玉柱	中南大学	Fast packet classification in firewall using unit space cuttings
		卢振平	解放军信息工程大学	一种针对软件定义网络的安全控制器调度时间机制
		杜红乐	商洛学院	基于协同半监督支持向量机的网络异常检测
		祝玉军	安徽师范大学	A rendezvous mechanism for energy balance in WSNs
		蔡赛华	中国农业大学	Exception detection of data stream based on improved maximal frequent itemsets mining
		齐　平	铜陵学院	一种基于图模型的可信云资源调度算法
		Gan Jin	Université de Franche-Comté	The LiSe Sense-Mining System
16:00-16:20	会议休息（茶歇）			
16:20-18:00	刘　强	崔朝阳	北京遥测技术研究所	适用于集群无人机的自组网安全分簇算法-UASCA
		邵国林	四川大学	The Analysis of Malicious Group Based on Suspicious Communication Behavior Aggregation
		王　龙	北京理工大学	Analysis of Vulnerability Correlation Based on Data Fitting
		吕伟栋	海军工程大学	一种基于树形拓扑结构的拜占庭容错系统设计
		陈松健	南京邮电大学	移动僵尸网络的命令与控制信息隐匿技术研究
		谈　诚	武汉大学	CAPT: Context-Aware Provenance Tracing for Attack Investigation
		曾雅丽	福建师范大学	Reliable Topology Control Algorithm in Cognitive Radio Networks
		王栋城	福建师范大学	基于身份盲签名的无线Mesh网络匿名切换认证方案
		王昱波	北京工业大学	A Trusted Routing Mechanism Suitable for the Sensing Nodes in Internet of Things
		朱文强	江西财经大学	A trustworthy group identifying trust metric for Peer-to-Peer service sharing economy based on personal social network of users

Session8：内容安全与应用安全　时间：9 月 16 日下午　地点：第九会议室

时间	主持人	报告人	单　位	题　　目
13:30-16:00	熊金波	董祥祥	中科院	动态社会网络数据发布隐私保护方法
		王丽娜	武汉大学	A new blind detection approach for JPEG image steganalysis
		刘明明	武警工程大学	一种基于浅层卷积神经网络的隐写分析方法
		马　蓉	福建师范大学	基于博弈论的隐私保护方法研究综述
		詹　静	北京工业大学	TPTVer: A Trusted Third Party based Trusted Verifier for Multi-Layered Outsourced Big Data System in Cloud Environment
		孙泽锐	广西财经学院	基于插值图像的可逆信息隐藏算法
		阮树骅	四川大学	A Metric Model for Cloud Computing Security Risk Assessment
		罗　鹏	武警工程大学	A Print-scan Resilient Watermarking Algorithm in NSCT Domain based on Digital Holography
		齐法制	中国科学院高能物理研究所	The trusted virtual machine cluster construction method based on particle wave equation
		林　英	云南大学	The Design and Implement of Spatial Grid Quadtree Based Hilbert Location K-Anonymity Algorithm
16:00-16:20	会议休息（茶歇）			
16:20-18:00	马行空	樊佩茹	武汉大学	APM：一种 IaaS 云可信性测试环境中的 Agent 保护机制
		孙　亮	中电科技（北京）有限公司	The Research of Secure Startup Mechanism of Server Based on Trusted BMC
		李怡佳	武汉大学	TBStacker：一种基于可信前台任务栈序列的 Android Activity 劫持防护框架
		李　伟	西安电子科大	An efficient ID-based mutual authentication and key agreement protocol for mobile multi-server environment without a trusted registration center and ESL attack
		佘　维	郑州大学	Micro-payment Real-time Trading Strategy Optimization Method in Blockchain Based on DCPN
		陈锦富	北京系统工程研究所	A vulnerability model construction method based on chemical abstract machine
		何婷婷	北京理工大学	Research on malicious code analysis method based on semi-supervised learning
		汪　润	武汉大学	SPRD：一种面向大规模 Android 重打包应用的准确检测方法

会议特邀报告一

报告人：Robert H. Deng

题　目：Techniques for End-to-End Security in Mobile Computing

Robert H. Deng，新加坡管理大学教授，博士生导师， IEEE Fellow。1985 于美国 Illinois Institute of Technology 获博士学位，自 1987 年 7 月起先后在新加坡国立大学、新加坡国家科研局、新加坡管理大学工作，曾任新加坡国家科研局信息通信研究所(I2R)信息安全首席科学家。先后在《IEEE Transactions on Information Theory》、《ACM Transactions on Information and System Security》、IEEE Symposium on Security and Privacy（IEEE S&P）、 ACM Conference on Computer and Communications Security（ACM CCS）等国际期刊和国际会议发表了 200 多篇论文,论文被引用 6000 多次。拥有 26 项国际专利，并有 2 项发明被 ISO/IEC 采纳为国际标准。担任过 100 多次国际会议（包括 IEEE S&P、ACM CCS、ASIACRYPT、ESORICS 等顶级国际会议）的程序委员会委员、程序委员会主席、程序委员会主席或大会主席，应邀在近 30 个国际会议上作特邀报告。担任 7 个国际期刊的副主编或编委(其中担任《IEEE Transactions on Dependable and Secure Computing》和《IEEE Transaction on Inform. Forensics and Security》副主编)。曾获 2010 年亚太信息安全领袖成就奖、NDSS2012 卓越论文奖等多项奖励。

会议特邀报告二

报告人：贾小华

题　目：Security and Privacy Assurance in Cloud Storage and Crowdsourcing Systems

贾小华，香港城市大学教授，哈尔滨工业大学深圳研究生院教授，博导、“长江学者奖励计划”特聘教授,“千人计划”国家特聘专家、IEEE Fellow. 1986 年获取中国科技大学计算机科学理科硕士学位，1991 年获取日本东京大学信息科学理科博士学位，先后在澳大利亚昆士兰州大学、香港城市大学任教职，香港城市大学科学与工程学术与学位委员会主席。在分布式系统、计算机网络等方面的研究成果卓著，发表论文 130 余篇，其中 SCI 索引 50 余篇。担任国际杂志 Journal of Combinatorial Optimization (Kluwer Academic Pub) 的编委，Special Issue on Cluster Computing on the Internet, Cluster Computing: A Journal of Computer Software and Communications (Baltzer Pub) 和 Special Issue on Web Servers and Content Distribution Networks (CDN), Journal of World Wide Web: Internet and Web Information Systems (Kluwer Academic Pub) 的客座编委，是关于分布式系统和计算机通讯方面的很多国际会议的组委会成员或者主席。

会议特邀报告三

报告人：杜跃进

题　目：新安全中的几个重要问题及其应对思路

杜跃进，阿里巴巴集团安全部技术副总裁、首席安全专家，博士，教授，中国网络空间安全协会副理事长，中国通信标准化协会副主席，中国保密协会个人隐私保护专委会副主任，中国计算机学会计算机安全专业委员会常务委员，中国互联网协会网络与信息安全工作委员会副主任委员。曾任网络安全应急技术国家工程实验室主任、国家网络信息安全技术研究所所长、国家计算机网络应急技术处理协调中心（CNCERT/CC）副总工程师，亚太计算机应急响应组织（APCERT）副主席、杭州G20、北京奥运、上海世博、广州亚运会安保工作组专家。在我国最早开展国家级网络安全事件的监测分析和应急响应，并在我国互联网应急体系建设和国际合作方面作了大量工作；完成多项国家级科研项目，作为课题副组长研制建设了我国的国家级网络安全基础设施。曾两次获得国家科技进步一等奖，获得新世纪百千万人才工程国家级人选、全国青年岗位能手、信息产业十大杰出青年等荣誉称号，获得国务院特殊津贴。

会议特邀报告四

报告人：张方国

题　目：区块链-理论与应用

张方国，中山大学数据科学与计算机学院的教授、博士生导师。中山大学网络空间安全系主任，中山大学网络空间安全研究所所长，广东省信息安全技术重点实验室副主任，中国密码学会常务理事，广东省国家保密局保密技术专家委员会委员，广东省涉密信息系统分级保护测评专家委员会委员，广东省计算机学会信息安全专委会副主任委员。担任《密码学报》、《信息网络安全》(2014-2017)杂志编委，Pairing 2013，ProvSec2009，JWIS2011 和 AsiaJCIS 2012-13 的程序委员会联合主席，AsiaJCIS14-16 指导委员会委员，中国科协第 265 届青年科学家论坛联合执行主席，以及一百多个密码学领域国内外学术会议的程序委员会委员。在密码学研究领域的短签名，双线性对快速计算，椭圆曲线离散对数问题计算等方面做出了一些有创新性的工作，发表论文 180 多篇，其中 SCI 文章 100 多篇，包括《IEEE Transactions on Information Theory》和 AsiaCrypt 等多个国际权威刊物和密码学顶级会议，申请国内外专利 13 项。

会议特邀报告五

报告人：窦强

题　目：飞腾 CPU 实践与体会

窦强，研究员，博士生导师，现任国防科技大学计算机学院微电子与微处理器研究所所长，银河/天河工程副总设计师。总体负责飞腾自主高性能微处理器和专用微处理器研制。在高性能计算机系统结构与高端芯片设计验证技术方面取得大量技术突破，解决超大规模一致性协议、多核微处理器快速验证和超高性能 CPU 新型架构等重大问题。先后负责完成核高基国家科技重大专项 2 项，在研 1 项；同时主持并参与国家自然科学基金项目，863/973 重大专项。主持完成自主高性能的多核 CPU 芯片 FT2000、FT1500A、FT-1000A，并在国产化信息系统中大范围推广，解决我国信息化过程中的国产化关键问题。先后获得国家科技进步特等奖 1 项，一等奖 1 项，军队科技进步奖 3 项，中国计算机学院科学技术奖一等奖 1 项。入选国家百千万人才工程，入选高层次科技创新人才工程学科拔尖人才培养对象，荣获十八届“求是奖”。

会议特邀专题一：自主与可控信息技术

报告人：戴华东

题　目：麒麟操作系统的实践与思考

戴华东，男，国防科技大学计算机学院国产基础软件工程研究中心副主任。担任银河麒麟操作系统副总设计师，长期从事高性能计算机操作系统和通用服务器、桌面操作系统的研制工作，在麒麟国产操作系统方面做出了较大贡献。获军队科技进步一等奖 1 项，二等奖 2 项，省部级科技进步一等奖 2 项。在国内外期刊和会议上发表论文 30 余篇，出版专著 1 部，获发明专利授权 10 余项。

报告人：王宝生

题　目：以新思路应对网络空间安全挑战

王宝生，男，研究员，国防科技大学计算机学院网络与信息安全研究所所长、博士生导师，主要研究方向计算机网络体系结构、网络安全、高性能网络设备等，曾参加过我国第一台核心路由器研制。

报告人：孙家彦

题　目：云数据库技术对可信计算的支持

孙家彦，毕业于北京大学电子学系，从事软件研发、系统构架、项目管理、互联网产品设计及运营等相关工作近 20 年，其中从事企业经营管理 10 年以上，在企业战略规划领域有深厚的理论功底和丰富的运作经验，在企业管理、项目管理、互联网推广运营等多个方面经验丰富。现任北京优炫软件股份有限公司董事、COO。

会议特邀专题二：互联网安全威胁与防范

报告人：魏强

题　目：未知的博弈--威胁向量分析与防御

魏强，解放军战略资源部队信息工程大学副教授，博士生导师，享受军队优秀技术人才岗位津贴，计算机病毒防御国家工程实验室专家委员会专家委员，自动化学会工业控制系统信息安全专家委员会专家委员，中国国家漏洞库首批特聘专家，中国网络安全产业联盟技术创新专业委员会专家委员。

报告人：张悦

题　目：勒索病毒攻防漫谈

张悦，男，暨南大学网络空间安全学院博士，研究方向系统安全、恶意代码检测、区块链等，取得了一些突出的研究成果。2016 年 5 月，曾对目前主流云盘进行过安全性测试，发现多个网盘存在安全性问题，成果被中央电视台专题报道，并被各大媒体转载。曾攻破某国外著名社交软件登录认证系统，发现了某知名支付系统的界面劫持漏洞，参与设计了 WannaCry 勒索病毒查杀工具。

报告人：肖晟

题　目：“弱”密码的阴影-猜测密码攻击的一些进展

肖晟，男，湖南大学信息科学与工程学院院长助理，CCF/IEEE/ACM 会员，湖南省计算机学会理事，ACM 中国区教育分会理事，主要研究方向为网络通信安全，高性能计算，数据分析与可视化。自 2013 年取得美国 UMass Amherst 博士学位回国以来，主持和参与了国家自然科学基金、“核高基”、部委重点研发课题等科研项目十余项，发表了二十余篇 CCF 列表内的国际会议和期刊论文，在 Springer 出版社出版专著 1 部。

会议特邀专题三：企业创新技术

报告人：唐宏斌

题　目：云虚拟化安全

唐宏斌，博士，蓝盾教育研究院副院长，毕业于电子科技大学，研究方向为密码学及网络安全,在国内外的信息安全领域重要学术期刊和会议上发表论文12篇(多篇论文被SCI检索)，致力于网络安全实训产品规划和研发工作。

报告人：刘冬梅

题　目：国际可信计算的愿景和创新战略

刘冬梅，博士，微软可信赖计算部网络空间安全技术总监，负责微软中国可信赖计算等安全策略的制定与推广、与国内安全社区和研究院所的项目合作，推进微软可信赖计算技术在中国的应用和实践。拥有信息安全行业十余年的从业经验，曾任多届ICICS国际会议出版主席，在国内重要刊物发表论文10余篇，编辑论文集两部，发明专利4项。

会 议 须 知

一、会务组

总　　负　　责：付绍静（15526404186）

会议住宿餐饮：范　雯（13487317813）

会 议 接 送：宁伟勋（13786124543）

会 议 财 务：王　丰（13739071153）

二、会务费及食宿

论文作者注册费为1500元人民币，普通代表提前注册会议费1300元、现场注册收取会议费1600元。 住宿地点为湖南长沙现代凯莱大酒店，代表在酒店总台自行办理手续。在酒店住宿的代表凭房间自带早餐券就餐，在外住宿的代表请自行安排早餐。会议期间中餐和晚餐，代表凭会议餐券在酒店自助餐厅就餐（15日晚餐为围桌晚宴）。

三、友情提醒

1. 会议期间，请您佩戴代表证出入酒店、参加会议、用餐及参加活动。

2. 请各位代表妥善保管餐券、会议资料，严防丢失。

3. 请按时就餐，会议期间统一行动，确保安全。晚上外出最晚23：00以前返回酒店，特殊情况与会务组联络。