第十二届中国可信计算与信息安全学术会议

The 12th Chinese Conference on Trusted Computing & Information Security

CTCIS2018 程序册

湖北武汉　2018.10

CTCIS 2018 组织机构

主办单位: 中国计算机学会

承办单位: 武汉大学

中国计算机学会容错计算专业委员会

赞助单位: 大唐高鸿信安（浙江）信息科技有限公司

国际可信计算组织大中华区工作组

大会主席:

沈昌祥，中国工程院院士

大会副主席:

张焕国，武汉大学 教授

程序委员会主席:

赵　波，武汉大学 教授

程序委员会副主席:

严　飞，武汉大学 副教授

组织委员会:

余发江，武汉大学 副教授

沈志东，武汉大学 副教授

王张宜，武汉大学

王后珍，武汉大学

张立强，武汉大学

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

黄继武　　深圳大学

荆继武　　中科院信息工程研究所

李建华　　上海交通大学

刘建伟　　北京航空航天大学

李舟军　　北京航空航天大学

马建峰　　西安电子科技大学

秦志光　　电子科技大学

苏金树　　国防科技大学

石文昌　　中国人民大学

王清贤　　信息工程大学

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
陈恺	中国科学院信工所
程庆丰	信息工程大学
杜瑞忠	河北大学
冯秀涛	中科院系统科学研究所
付绍静	国防科技大学
付伟	海军工程大学
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
胡卫	海军工程大学
胡玉鹏	湖南大学
黄琼	华南农业大学
林莉	北京工业大学
羌卫中	华中科技大学
秦宇	中科院软件所

屈龙江	国防科技大学
邵俊	浙江工商大学
孙磊	信息工程大学
唐明	武汉大学
滕少华	广东工业大学
田东海	北京理工大学
童言	华中农业大学
王伟	北京交通大学
王文贤	四川大学
王志波	武汉大学
伍前红	北京航空航天大学
鲜明	国防科技大学
肖亮	厦门大学
徐明迪	中船重工 709 研究所
徐鹏	华中科技大学
叶登攀	武汉大学
张建标	北京工业大学
赵磊	武汉大学
周学广	海军工程大学
周亚金	浙江大学
邹德清	华中科技大学
朱辉	西安电子科技大学

会议议程一览表

日期	时间	内容			地点
10 月 18 日	13:00—22:00	参会代表报到、注册			光谷金盾大酒店前台
	20:30—21:30	程序委员会扩大会议			3F 东湖厅
10 月 19 日	9:00—9:20	开幕式	主持人：张焕国教授	领导、嘉宾致辞	3F 大宴会厅
	9:20—10:00	特邀报告 1：	主持人：石文昌教授	可信计算 3.0 发展与创新 报告人：沈昌祥 中国工程院院士	3F 大宴会厅
	10:00—10:20	集体合影			酒店门口
	10:20—10:40	茶歇			廊区
	10:40—11:20	特邀报告 2	主持人：田俊峰教授	量子信息技术原理与进展 报告人：韩正甫 中国科技大学教授	3F 大宴会厅
	11:20—12:00	特邀报告 3		拥抱大数据时代——FAST 海量天文大数据计算 报告人：谢晓尧 贵州师范大学副校长	
	12:00—13:30	自助午餐			3F 派瑞阁西餐厅
	13:30—16:00	分论坛	密码学 I		3F 大宴会厅 1 厅
			网络安全 I		3F 大宴会厅 2 厅
			系统安全 I		3F 大宴会厅 3 厅
			内容安全		3F 琴台厅
			软件学报 I		3F 晴川厅
	16:00—16:15	茶歇			廊区

	16:15—18:15	分论坛	密码学 II		3F 大宴会厅 1 厅
			网络安全 II		3F 大宴会厅 2 厅
			系统安全 II		3F 大宴会厅 3 厅
			优秀论文评选		3F 琴台厅
			软件学报 II		3F 晴川厅
	18:30—20:00	欢迎晚宴			2F 会议厅 2+3 厅
10 月 20 日	9:00—9:40	特邀报告 4	主持人：张建标教授	移动目标防御技术研究进展 报告人：张红旗 信息工程大学教授	3F 大宴会厅
	9:40—10:20	特邀报告 5		阿里云安全实践 报告人：牛纪雷 阿里云安全总监	
	10:20—10:40	茶歇			廊区
	10:40—11:20	特邀报告 6	主持人：韩伟力教授	展望人工智能密码——从演化密码到量子人工智能密码 报告人：王潮 上海大学教授	3F 大宴会厅
	11:20—11:40	特邀报告 7		物联网设备安全和设备标识组合引擎 报告人：刘冬梅 微软可信赖计算部网络空间安全技术总监	
	11:40—12:00	特邀报告 8		可信软件版权保护系统介绍 报告人：李业旺 大唐高鸿信安可信计算产品架构师	
	12:00—13:30	自助午餐			3F 派瑞阁西餐厅
	13:30—16:00	分论坛	密码学 III		3F 大宴会厅 1 厅
			网络安全 III		3F 大宴会厅 2 厅
			系统安全 III		3F 大宴会厅 3 厅

			隐私保护	3F 琴台厅
	16:00—16:15	茶歇		廊区
	16:15—18:15	分论坛	密码学 IV	3F 大宴会厅 1 厅
			网络安全 IV	3F 大宴会厅 2 厅
			系统安全 IV	3F 大宴会厅 3 厅
			可信计算工业技术研讨	3F 琴台厅
	18:30—20:00	自助晚餐		3F 派瑞阁西餐厅
10 月 21 日	8:30—11:30	自由研讨		酒店门口乘车
	12:00—13:30	午餐		

会议特邀报告一

报告人：沈昌祥

题　目：可信计算 3.0 发展与创新

沈昌祥，浙江奉化人，中国工程院院士，1965 年毕业于浙江大学，从事计算机信息系统、密码工程、信息安全体系结构、系统软件安全（安全操作系统、安全数据库等）、网络安全等方面的研究工作。先后完成了重大科研项目二十多项，取得了一系列重要成果，曾获国家科技进步一等奖 2 项、二等奖 2 项、三等奖 3 项，军队科技进步奖十多项。这些成果在信息处理和安全技术上有重大创造性，多项达到世界先进水平，在全国全军广泛应用，取得十分显著效益，使我国信息安全保密方面取得突破性进展。 在网络安全和科技创新、咨询论证和学科专业建设、人才培养等方面做出了杰出贡献。1988 年被授予“海军模范科技工作者”荣誉称号，曾当选为七届全国人大代表，1995 年 5 月当选为中国工程院院士，1996 年获军队首届专业技术重大贡献奖，2002 年荣获国家第四届"光华工程科技奖" ，2016 年获首届中国网络安全杰出人才奖。目前担任国家信息化专家咨询委员会委员，国家三网融合专家组成员，国家集成电路产业发展咨询委员会委员，国家保密局专家咨询委员会主任委员，国家信息安全等级保护专家委员会主任委员，国家密码管理委员会办公室顾问，公安部特聘专家，中国人民银行信息安全顾问，国家税务总局信息技术咨询委员会委员。同时还担任北京大学、国防科技大学、浙江大学、中科院研究生院、上海交通大学等多所著名高校的博士生导师。

内容简介：

没有网络安全就没有国家安全，当前美国垄断网络空间霸权的格局没有根本

改变，网络空间敌强我弱的态势没有根本改变，敌对势力利用网络“扳倒中国”的图谋没有根本改变，核心技术受制于人的局面没有根本改变。安全是发展的前提，发展是安全的保障。没有网络安全，信息社会将成为黑暗中的废墟。因此，必须树立科学的网络安全观。本报告将首先向听众阐述什么是科学的网络安全观，解释为什么需要主动免疫可信计算，然后介绍中国可信计算有哪些革命性的创新，最后给出如何使用可信计算解决受制于人的困境的思路，以及可信计算在国家重要部门的成功应用案例。

会议特邀报告二

报告人：韩正甫

题　目：量子信息技术原理与进展

韩正甫，男，安徽寿县人，1962 年生。教授，博士生导师；中国密码学会常务理事，量子密码专业委员会副主任。 1987 年后，师从中国科技大学郭光灿院士研究量子信息技术，2001 年我国第一个完成地下 6.4 公里量子密钥分配实验，2005 年完成北京--天津 125 公里国际最远的量子密钥分配实验，2007 年发明量子路由器，完成国际上第一个全通型量子密钥通信网络，2009 年国际上第一个将量子密码技术与实际应用结合，实现“量子政务网”。在长程光纤量子密钥分配原理与系统及应用、量子信息器件、量子密钥分配稳定性，量子密码网络、光学微腔 QED 等方面取得了一系列成果，拥有多项本领域基础性的国内和国际专利。已在 Nature Photonics， Nature Communication，美国物理评论系列（PRL、PRA、PRB 等）、物理联合会系列（APL 等）、光学学会系列（OL、OE、JOSA、AO、OC 等、电气和电子工程师协会系列（IEEE- TIT、PTL）等国内外杂志发表论文 200 多篇，他引 3000 余次；曾获得国家重大基础研究计划（973 计划）先进个人，安徽省自然科学一等奖（第一），教育部技术发明一等奖（第一），军队科技进步一等奖（第一）等。

内容简介：

从量子信息技术的原理及其本质入手，重点讲述量子信息与经典信息的异同，阐述量子信息的优势及未来的可能走向；介绍量子密钥分配原理及其组网应用思路和趋势；简述量子计算机的当前发展状况，展示量子信息技术的发展前景。

会议特邀报告三

报告人：谢晓尧

题　目：拥抱大数据时代——FAST 海量天文大数据计算

谢晓尧，贵州省最高科技技术奖获得者，贵州省政协原副主席，贵州师范大学副校长，贵州省首批省管专家，贵州省核心专家，享受国务院特殊津贴，贵州省大数据专家組副长。主持完成了国家 863 专项课题及贵州省多项攻关项目。获得贵州省最高科学技术奖，贵州省科技进步一等奖 1 项、二等奖 4 项、三等奖 4 项、贵州省教学成果特等奖 1 项、出版专著及教材 9 部，发表论文 114 多篇。谢晓尧教授成为贵州 IT 界的先行者和推动者。

内容简介：

本报告首先简单介绍 FAST（500 米球面射电望远镜）系统，然后介绍 FAST 大数据处理，同时介绍大数据处理中的信息安全问题，最后介绍 FAST 大数据处理对我们挑战和机遇。

会议特邀报告四

报告人：张红旗

题　目：移动目标防御技术研究进展

张红旗，男，信息工程大学教授，博士生导师，河南省信息安全重点实验室副主任。教育部高等学校信息安全专业教学指导委员会委员，国家网络安全优秀教师，河南省高等学校教学名师。曾获国家教学成果二等奖、国家科技进步二等奖等多项奖励，主编国家级规划教材多部。

内容简介：

移动目标防御是一种改变游戏规则的主动防御技术。主要介绍移动目标防御产生的背景、概念，移动目标防御的设计原则与系统架构；移动目标防御策略制定、变换机制、效能评估等移动目标防御关键技术；移动目标防御技术在传统网络、SDN 网络等场景应用。

会议特邀报告五

报告人：牛纪雷

题　目：阿里云安全实践

牛纪雷，阿里云安全总监，主要负责阿里云云计算、大数据、IoT、AliOS 安全。

内容简介：

云计算做的就是信任，安全是信任的基础。阿里云经过多年的发展，在云计算安全上耕耘多年。牛纪雷作为阿里云安全总监，见证和搭建了阿里云的云计算安全体系，此次分享将向大家介绍阿里云在云计算安全领域的安全实践。

会议特邀报告六

报告人：王潮

题　目：展望人工智能密码——从演化密码到量子人工智能密码

王潮，上海大学教授/博导。主要研究方向椭圆曲线密码、网络安全、量子人工智能密码设计与分析。现任 IEEE China Council（中国理事会）副主席，中国人工智能学会理事，中国电子学会信息安全专家委副主任委员，中国计算机学会容错专委会常务委员，第六届上海市信息化专家委成员。曾负责电信级 IP 综合网络管理产品研发，列入科技部国家级重点科技成果。是第二届中国电子学会全国优秀科技工作者。

内容简介：

在演化密码思想理论基础上，拓展到量子人工智能密码，采用 D—wave 真实量子计算机完成国际上首次密码设计实验，采用 Dwave 的量子人工智能原理优化对 RSA 公钥密码的攻击，实验结果超过目前公开文献其他量子计算分解整数的规模。最后展望演化密码思想融合人工智能方法对密码部件设计、密码分析的作用，降低密码分析的时间复杂度数量级，实现一次一密码算法。

会议特邀报告七

报告人：刘冬梅

题　目：物联网设备安全和设备标识组合引擎

刘冬梅，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，旨在增进微软与国内安全社区、研究院所以及产业界的合作，推进国际最佳安全技术实践在中国的应用。于 2010 年获得信息安全工学博士学位，拥有信息安全行业十余年的从业经验，作为技术骨干和项目组核心成员曾参加多项国家科技重大专项的研发，曾任多届 ICICS 国际会议出版主席，在国内重要刊物和国际会议上发表论文 10 余篇，编辑论文集三部，发明专利 4 项。

内容简介：

随着物联网的发展，联网设备几乎被应用到工业的每个领域，但是随着物联网应用场景的拓展，利用这些联网设备的网络攻击亦呈现快速增长的趋势。在许多情况下，这些攻击不仅给设备制造商造成了严重的经济损失，也给客户带来了严重的信息安全隐患。没有哪个系统设计师想要成为那个负责发布一个被黑客入侵的设备的人。现在每个工程师都意识到安全必须是连接产品设计的一个基本组成部分。

为了满足增加安全性的需求，特别是在受限的环境中设备安全性的需求，TCG 与成员公司合作开发了 DICE（设备标识符组成引擎）体系结构。DICE 具有以下特性:

1、基本安全物联网成本接近于零

2、简单硬件需求使得 DICE 能适应大多数任何系统或组件

3、提供基于硬件的身份和认证,以及密封、数据完整性,设备恢复和更新

DICE 体系结构已被开发，以提供独特的设备标识，保护车辆的数字内容和对其控制系统和敏感数据的访问。任何嵌入式系统，特别是那些成本敏感但仍然需要增强安全性和惟一标识的系统，都可以通过实现 DICE 体系结构而获益。TCG 开放与芯片制造商和产业链其他厂商合作，建立独特的硬件基础安全能力，将安全嵌入到他们物联网设备的 DNA 中。

会议特邀报告八

报告人：李业旺

题　目：可信软件版权保护系统介绍

李业旺，大唐高鸿信安可信计算产品架构师。曾就职于多家国际知名 IT 企业，具有十多年研发实践经验，擅长于操作系统、信息安全技术、近年来专注于可信计算领域，带领团队开发了一系列可信计算产品，同时，紧密关注人工智能、区块链等有应用场景的安全问题，致力于用可信计算技术为相关应用提供全面、完整、高级别的安全保护。

内容简介：

世界各国都对知识产权的保护工作非常重视，均通过法律法规结合防盗版等手段对相关成果进行保护。但随着人工智能、区块链等新兴技术的出现，这类凝聚企业智力成果，以软件为主要载体的知识产权的保护难度愈发增大，仅仅依靠法律法规很难对相关成果进行卓有成效的保护，软件盗版、数据泄露等事件经常发生，不但损害用户的利益，也对企业知识产权造成危害。大唐高鸿信安基于可信计算技术开发的可信软件版权保护系统可以从软件的静态存储和动态运行两方面对软件本身及重要数据进行软硬一体全时保护，全面提升软件的安全性，保护企业知识产权免受侵害。

分会场安排

分会场 1：密码学 I		时间：10 月 19 日下午		地点：3F 大宴会厅 1 厅
时间	主持人	报告人	单位	题目
13:30—16:00	付绍静	陈林	武警工程大学	基于粒子群算法的一种新型能量分析模型
		姚萌萌	江南计算技术研究所	一种改进的基于认证测试的形式化分析方法
		李明明	信息工程大学	Impossible Differential Cryptanalysis of SPECK
		刘凯	四川大学	Password Guessing Based on Semantic Analysis and Neural Networks
		贾建卫	华为技术有限公司	Cryptanalysis of ElGamal-like cryptosystem based on matrices over groupring
		王蓉蓉	西安邮电大学	GF(3^m)上 Hessian 曲线的三进制 Montgomery 算法
		张键红	北方工业大学	基于区块链的匿名密码货币支付协议
		白海艳	陕西师范大学	共享秘密上的量子计算
16:00—16:15	茶歇			
分会场 1：密码学 II		时间：10 月 19 日下午		地点：3F 大宴会厅 1 厅
时间	主持人	报告人	单位	题目
16:15—18:15	张建标	卢士美	西安邮电大学	GF(2^m)椭圆曲线上的 Co_Z 点加算法
		王南	辽宁工业大学	一种改进的防窃听 LT 码
		武迪	北京航空航天大学	集成消息填充的 SM3 算法硬件设计与实现
		赵建	信息工程大学	Ciphertext-policy attribute-based encryption for circuits from lattices under weak security model

		付雨萌	信息工程大学	An efficient and revocable decentralizing attribute-based encryption for mobile cloud computing
		魏铎	信息工程大学	A Predicate Encryption Scheme with Adaptively Secure
		向广利	武汉理工大学	Aggregation Tree Statistical Computing Based on Functional Encryption
		杨敏	武汉大学	New AES Dual Ciphers Based On Rotation of Columns

分会场 2：网络安全 I		时间：10 月 19 日下午		地点：3F 大宴会厅 2 厅
时间	主持人	报告人	单位	题目
13:30—16:00	徐洋	宋贺	江南大学	基于轻量级虚拟化的 LDDoS 仿真技术
		贺玉鹏	河北大学	SDN 环境下的 DDoS 攻击检测方案
		张希鹏	北京工业大学	Sensing Layer Network Resource Allocation Model Based on Trusted Groups
		刘建利	北京工业大学	A multilevel trusted clustering mechanism for the awareness layer of the Internet of things
		王昱波	北京工业大学	A Behavioral Measurement Model Suitable for the Sensing Nodes of Internet of Things
		谢丽霞	中国民航大学	链路洪泛攻击的 SDN 移动目标防御机制
		王文胜	河北大学	一种 SDN 控制节点故障恢复的部署策略
		郭蕊	武汉大学	A multi-layer virtual network isolation detection method for cloud platform
		王斐	武汉大学	面向 SDN 的安全威胁及其对抗技术研究
16:00—16:15	茶歇			
分会场 2：网络安全 II		时间：10 月 19 日下午		地点：3F 大宴会厅 2 厅
时间	主持人	报告人	单位	题目
16:15—18:15	公备	蔡赛华	中国农业大学	An efficient outlier detection approach over data stream based on minimal weighted rare pattern mining
		郝耀军	燕山大学	An ensemble detection method for shilling attacks based on

				features of automatic extraction
		金渝筌	中国工程物理研究院电子工程研究所	一种基于通信相似度的僵尸网络节点检测方法
		王子晔	中共中央办公厅电子科技学院	Network Security Situation Evaluation Method Based on Alert Verification and Fuzzy Reasoning
		文奕	四川大学网络空间安全学院	面向安全分析的大规模网络下的 DNS 流量还原
		何涛	四川大学	基于告警属性相似度聚类的攻击场景关联规则挖掘方法研究
		张思聪	贵州师范大学	基于 dCNN 的入侵检测方法
		康海燕	北京信息科技大学	基于网络日志的用户行为刻画与预测研究

分会场 3：系统安全 I		时间：10 月 19 日下午		地点：3F 大宴会厅 3 厅
时间	主持人	报告人	单位	题目
13:30—16:00	韩伟力	赵鹏远	武汉大学	A Lightweight Double Identity Verification Using PUFs
		刘秀文	武汉大学	面向人机交互场景的信息欺骗分类及其威胁抑制
		金银山	武汉大学	基于深度学习的恶意样本检测
		朱泽瑾	武汉大学	Windows UAC 机制缺陷研究
		徐来	武汉大学	Memway: In-Memory Waylaying Acceleration for Practical Rowhammer Attacks Against Binaries
		熊鑫立	陆军工程大学	基于系统攻击面的动态目标防御有效性评估方法
		吕从东	南京审计大学	Noninterference Models of Cloud Computing Security
16:00—16:15	茶歇			
分会场 3：系统安全 II		时间：10 月 19 日下午		地点：3F 大宴会厅 3 厅
时间	主持人	报告人	单位	题目
16:15—18:15	孙磊	梅戌芬	武汉大学	一种基于 JavaScript 直接执行的 Chrome 扩展动态分析方法
		常天天	四川大学	面向 Hive 的基于安全域的数据隔离保护框架
		胡俊	北京工业大学	vTCM ：一种基于物理可信计算环境虚拟化的虚拟可信密码模块
		孙亮	中电科技（北京）有限公司	基于 UEFI 的固件级硬盘安全保护机制研究
		黄坚会	北京工业大学	TPCM 主动防御可信服务器平台设计
		高雪原	中国船舶重工集团公司第七 0 九研究所	An Approach of Implementing SW-TPM in Real-Time Operating System
		肖欢	四川师范大学	一种虚拟货币热钱包的可信保护方案

分会场 4：内容安全		时间：10 月 19 日下午		地点：3F 琴台厅
时间	主持人	报告人	单位	题目
13:30—16:00	叶登攀	石朋亮	河北大学	Dynamic Multiple Copies Adaptive Audit Scheme Based on DDCT
		杨瀚溢	武汉大学	基于最小失真代价的 SILK 基音域自适应隐写算法
		王雪梅	四川大学	基于标签和分块特征的新闻网页关键信息自动抽取研究
		王培名	四川大学	多策略融合的微博数据获取技术研究
		梁英	中科院计算所	基于文本和链接的用户敏感属性迭代识别方法
		刘佳	武警工程大学	生成对抗网络在图像隐写中的应用
		孔咏骏	武警工程大学	基于序列自适应分离的 PVO 可逆信息隐藏算法
		刘佳	武警工程大学	Steganography Security: Principle and Practice
		彭菓玉	武警工程大学	一种基于纠错码的密文域可逆信息隐藏方法
16:00—16:15	茶歇			
分会场 4：优秀论文评选		时间：10 月 19 日下午		地点：3F 琴台厅
时间	主持人	报告人	单位	题目
16:15—18:15	王潮	陈思宇	西安电子科技大学	一种面向低轨卫星网络的用户随遇接入认证协议
		王锴	武汉大学	Leakage is Prohibited: Memory Protection Extensions Protected Address Space Randomization
		尚涛	北京航空航天大学	基于等差隐私预算分配的大数据决策树算法
		赵中楠	哈尔滨理工大学	Research on Fault Repair Method of All-optical Network based on SDN
		吴力强	武警工程大学	New Identity based Proxy Re-Encryption Scheme from Lattices

		马川	燕山大学	Communication-based Attacks Detection in Android Applications
		郝世荣	武汉大学	TVIDS : Trusted Virtual IDS With SGX

分会场 5：软件学报 I		时间：10 月 19 日下午		地点：3F 晴川厅
时间	主持人	报告人	单位	题目
13:30—16:00	张焕国 田俊峰 林璟锵	李明月	河北大学	基于倒排索引的可验证混淆关键字密文检索方案
		张帆	武汉轻工大学	基于无干扰的软件实时可信度量
		李明明	信息工程大学	Midori-64 算法的截断不可能差分分析
		唐奔宵	武汉大学	基于 Laplace 机制的普适运动传感器侧信道防御方案
		谭良	四川师范大学	基于 Duplication Authority 的 TPM2.0 密钥迁移协议及安全分析
16:00—16:15	茶歇			
分会场 5：软件学报 II		时间：10 月 19 日下午		地点：3F 晴川厅
时间	主持人	报告人	单位	题目
16:15—18:15	张焕国 田俊峰 林璟锵	徐林宏	信息工程大学	Piccolo 算法的相关密钥-不可能差分攻击
		刘明达	数字工程与先进计算实验室	基于区块链的分布式可信网络连接架构
		王文琦	武汉大学	一种面向中文文本情感倾向性检测的对抗样本生成方法
		李文婷	北京大学	无线传感器网络环境下多因素身份认证协议的内部人员攻击研究
		宋文纳	武汉大学	恶意代码演化与溯源技术研究

分会场 1：密码学 III		时间：10 月 20 日下午		地点：3F 大宴会厅 1 厅
时间	主持人	报告人	单位	题目
13:30—16:00	尚涛	戴千一	信息工程大学	分布式网络环境下基于区块链的密钥管理方案
		徐林宏	信息工程大学	Key-recovery attacks on LED-like block ciphers
		陈兰兰	华东交通大学	一种基于证书的短签名方案
		宋靖文	北京交通大学	一种改进的基于 SM2 的代理签名方案
		高凡	北京交通大学	基于 SM2 的无证书可截取签名方案
		张晓菲	郑州师范学院	An association ring signature for block chain e-money transactions
		吕从东	南京审计大学	货运列车车载网络轻量级身份认证协议研究
		刘金会	陕西师范大学	Lattice based double authentication preventing ring signature for security and privacy in Vehicular Ad-hoc Networks
		张业平	西安电子科技大学	一种面向无人机网络的密钥管理与认证协议
16:00—16:15	茶歇			
分会场 1：密码学 IV		时间：10 月 20 日下午		地点：3F 大宴会厅 1 厅
时间	主持人	报告人	单位	题目
16:15—18:15	朱辉	王子豪	湖北工业大学	一种高效的集合问题安全两方计算协议
		吴福生	贵州财经大学	基于密码协议实现的行为安全分析模型
		屈娟	重庆三峡学院	可证明的基于扩展混沌映射的匿名多服务器身份认证协议
		王利朋	郑州师范学院	A Voting Scheme in Blockchain Based on Threshold Group Signature

		杜杨	北京工业大学	A Fast Identity Authentication Solution for the Sensing Layer in Internet of Things
		陈立朝	西安科技大学	Two Anti-quantum Attack Protocols for Secure multiparty Computation
		张利华	华东交通大学	基于属性集合加密的云存储数据访问控制方案研究

分会场 2：网络安全 III		时间：10 月 20 日下午		地点：3F 大宴会厅 2 厅
时间	主持人	报告人	单位	题目
13:30—16:00	杜瑞忠	何旭东	中南民族大学计算机科学学院	网络协议流量识别综述
		宋元章	中国科学院长春光学精密机械与物理研究所	Detect peer-to-peer botnet with permutation entropy and adaptive information fusion
		崔艳	北京理工大学	基于 APT 网络行为分析的 Snort 规则扩展及 APT 检测的研究
		高洁	北京理工大学	Network Risk Assessment Method based on Asset Correlation Graph
		谢江维	北京理工大学	Detecting Malicious URLs using a Deep Learning approach based on Stacked Denoising Autoencoder
		郭守坤	北京理工大学	Research on Network Vulnerability Assessment Method Based on Zero-day Vulnerability Attack Diagram
		李丽	南京邮电大学	基于时滞的无线传感网恶意软件传播模型
		钟毅	四川大学网络空间安全学院	D-BitBot：基于比特币网络双向通信的 P2P 僵尸网络模型
16:00—16:15	茶歇			
分会场 2：网络安全 IV		时间：10 月 20 日下午		地点：3F 大宴会厅 2 厅
时间	主持人	报告人	单位	题目
16:15—18:15	徐明迪	林如姗	福建师范大学	认知无线电网络中基于接收信号强度的组密钥提取方案
		徐洋	贵州师范大学	基于 WiFi 大数据的区域人群轨迹模型
		朱瑞	福建师范大学	认知无线电网络中基于 SpaceTwist 的位置隐私保护方案

		陈雷	中国刑事警察学院	基于多层FGS视频编码的添加人工噪声无线安全多播策略
		代新敏	贵州大学	一种抗去同步的轻量级RFID双向认证协议
		卢政宇	信息工程大学	一种基于连续特征的未知协议消息聚类算法
		杨艳艳	郑州师范学院	Scheme on cross domain identity authentication based on group signature for cloud computing
		陈雨昊	南京邮电大学计算机学院	A novel shilling attack detection model for collaborative filtering recommender systems

分会场 3：系统安全 III		时间：10 月 20 日下午		地点：3F 大宴会厅 3 厅
时间	主持人	报告人	单位	题目
13:30—16:00	秦宇	户磊	四川大学	基于熵时间序列的恶意 office 文档检测技术研究
		陈铜	武汉大学	MOASB:基于内存对象访问序列的软件动态胎记及同源性判别方法
		赵佳利	北京交通大学	基于特征矩阵的 Python 克隆代码漏洞检测方法
		黎琳	武汉大学	基于 CNN 的 Webshell 文件检测
		韩静	北京交通大学	A Python security analysis framework in integrity verification and vulnerability detection
		周敏敏	江苏大学	A Method for Software Vulnerability Detection Based on Improved Control Flow Graph
		陈锦富	江苏大学	Predicting Vulnerable Software Components Via Bellwethers
16:00—16:15	茶歇			
分会场 3：系统安全 IV		时间：10 月 20 日下午		地点：3F 大宴会厅 3 厅
时间	主持人	报告人	单位	题目
16:15—18:15	谭良	樊佩茹	武汉大学	SIV: A Structural Integrity Verification Approach of Cloud Components with Enhanced Privacy and Performance
		阚哲	浙江师范大学	面向区块链环境的 CPS 系统可靠性分析
		姚维芊	武汉大学	一种基于手机传感器的定位伪造检测方案
		宋建涛	北京工业大学	A Trusted Measurement Model for Mobile Internet

		袁月	中国人民大学	Digging Evidence for Violation of Cloud Security Compliance with Knowledge Learned from Logs
		金鑫	四川大学	Cloud Virtual Machine Lifecycle Security Framework Based on Trusted Computing
		梁善强	西安邮电大学	基于 SEAndroid 的移动设备管理

分会场 4：隐私保护		时间：10 月 20 日下午		地点：3F 琴台厅
时间	主持人	报告人	单位	题目
13:30—16:00	孟庆树	熊星星	武汉大学计算机学院	基于局部差分隐私的电动汽车充电位置隐私汇聚
		杜波	武警工程大学（乌鲁木齐）	满足本地差分隐私的位置数据采集方案
		高志强	武警工程大学（乌鲁木齐）	基于粒子群优化的差分隐私模型拟合框架
		程楠楠	武汉大学计算机学院	用于敏感属性保护的(θ,k)-匿名模型
		于静洋	中国人民大学	HABKS: Hierarchical Attribute-based Keyword Search on Outsourcing Data
		刘新新	郑州师范学院	A Privacy Protection Scheme in VANETs Based on Group Signature
		肖衍行	北京信息科技大学	A Method for Time-series Location Data Publication Based on Differential Privacy
		王俊	中南民族大学	Differentially Private top-k Items based on Least Mean Square
16:00—16:15	茶歇			
分会场 4：可信计算工业技术研讨				地点：3F 琴台厅
时间	主持人	报告人	单位	题目
16:15—18:15	李彦	李彦	Intel	KPT/dHSM/SGX 英特尔相关技术
		刘鑫	国民技术	基于可信密码模块的的应用进展
		张岳公	三未信安	支持国密算法的 HSM 与 TPM 的融合和互补
		自由发言		

会议须知

一、会务组

总负责: 严飞（18986172798）

会议现场注册与住宿: 王后珍（13437279329）

会议餐饮：张立强（139713498644）

会场与场地设施：余发江（13797071569）

会务组在酒店一楼前台对面设置接待点：具体事宜可在接待点咨询

二、注册及食宿

10 月 10 日前注册费： 1500 元人民币

10 月 10 日后注册费： 1800 元人民币

现场注册费：1800 元人民币（仅提供安心付网络通道收费，现场不收取现金）

住宿地点：湖北武汉光谷金盾大酒店

代表在酒店按照会务组安排，在总台自行办理入住手续。

会议期间（19 日、20 日）中餐和晚餐，代表凭会议餐券在酒店自助餐厅就餐(19 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。