

# 4 基金 FOUNDATION

## 编者按

今天,移动互联网无处不在,人工智能已经向我们走来,“用代码改变世界”的流行语不再是程序员的自我调侃。现代信息社会对计算机系统的依赖,很大程度上体现为对软件的依赖,计算机系统的缺陷很多情况下都由软件问题引发。软件系统能否在操作错误、环境影响、外部攻击等干扰下,提供连续的服务,已成为一项严峻挑战。

为此,计算机科学家提出了软件“可信性”,这一在传统的可靠、可靠等概念基础上发展起来的新概念。早在十多年前,中国科学家分析认为,软件的运行环境和开发环境必将从传统的封闭、静态环境向开放、动态、多变的互联网环境转变,“可信软件”将成为现代软件技术发展和应用的重要趋势和必然选择。

2007年底,国家自然科学基金委员会启动了“可信软件基础研究”重大研究计划,投入经费1.9亿元,至2016年底结题。

该重大研究计划实施的十年间,研究人员以国家关键应用领域中软件可信性问题为主攻目标,既有力推动了软件基础理论的探索与创新,又有效应对了软件发展的重要科学挑战,对促进我国软件产业的振兴与发展具有重大的现实意义。同时,还形成了一支以中青年人才为主的高水平研究队伍,培养了一批站在世界科学研究前沿的学科带头人。

本期基金版将总结该重大研究计划取得的经验,介绍面向航天嵌入式软件、车联网及网络交易等三个行业的典型应用示范,充分展示该项目取得的成绩。

## 为网络交易保驾护航

■本报记者 甘晓

今天,以支付宝为代表的网络交易已经深入人们的日常生活。不确定的多样性业务需求导致网络交易软件系统的交易流程、实体和方式不断发生变化,而开放、动态网络环境使得网络交易软件系统面临着环境和恶意攻击手段的不可预知性。网络交易软件系统的安全可信问题逐步凸显。

在基金委“可信软件基础研究”重大研究计划的支持下,同济大学计算机系教授蒋昌俊带领团队面向网络交易支付,探究系统行为模式辨识和系统脆弱域辨识问题,创新性地提出了风险防控的行为分析技术与认证机制,建立了我国首个互联网交易风险防控体系及系统,解决了交易欺诈精准判定和瞬时辨识难题,成果在支付宝等得到成功应用。

研究人员注意到,人们在使用手机、电脑等工具进行网络浏览、购物时,有一些独特的习惯,会在网络支付平台留下蛛丝马迹。“这种习惯如同指纹一样难以复制,具有比密码更加复杂且细微的特点。”蒋昌俊介绍。

基于此,他带领团队通过采集和分析用户在系统中留下的痕迹,从用户在上网过程中对键盘的敲击行为以及网页浏览时间序列行为等方面构建用户行为证书,进行用户身份认证。设计了基于PN机制解析模型的交易行为认证机制,精准辨识交易欺诈,与支付宝合作研制了大规模分布式的交易支付风险实时防控平台与专用设备,



网络支付系统风险防控关键技术及其应用获2016年度国家科技进步奖二等奖

使得我国在该领域的技术水平处于国际领先,显著地提升了中国在互联网产业的国际地位。上述研究成果与支付宝合作获得2016年国家科技进步奖二等奖。

研究成果在支付宝、快钱等业内领先的第三方支付企业得到应用,服务200余个国家和地区的4亿多支付宝实名用户,系统交易放行率由原先的44%提高到96%,每次交易识别响应时间从200毫秒减少到100毫秒内,资金损失率下降到十万分之一以下。成果还为中国(上海)自由贸易试验区、国家电子商务综合创新实践区和中国工商银行等单位提供了重要技术支持。

## “可信软件基础研究”重大研究计划 为振兴软件产业提供科学支撑

■本报记者 甘晓



蒋昌俊(右一)在展示互联网交易风险防控成果



杨孟飞团队在进行小组研讨

## 让车联网更可信

■本报记者 胡璇子

近年来,随着社会经济的迅速发展,人们的出行需求与机动车保有量快速增长。公安部交管局数据显示,截至2018年6月底,我国机动车保有量达3.19亿辆。正如我们所见,道路上的车辆越来越多。车辆迅猛增长与道路环境承载能力之间突出的矛盾成为交通发展的瓶颈,“日常”的交通拥堵和高发的交通事故成为影响人们生活的重要问题。

综合来看,司机以个体的有限视野作为驾驶依据,缺乏对环境感知和全局信息的掌握,进而导致预警预判时间不足,出行决策不科学,是交通事故频发和事故发生的主要原因之一。

如何在有限的道路条件下,不断提升交通安全性和交通效率?将信息技术与交通有机结合,形成人车一路互联的车联网环境,为化解问题提供了有效手段。有预测认为,到2020年,全球90%以上的车辆都将具备联网能力。而作为典型的端-网-云一体化的复杂软件系统,车联网软件系统的可信程度,对交通的安全和效率有直接影响。

在基金委“可信软件基础研究”重大研究计划的支持下,北京航空航天大学课题组通过集成创新形成了一体化可信软件技术体系,并在车联网系统中进行了系统化示范应用,有效提升了车联网等网络应用软件系统的整体可信性。项目成果获得国家科技进步奖二等奖。

研究人员介绍,车联网软件具有开放性、规模性、演化性的特点,面临应用类型多样、应用规模快速变化、软件迭代更新

快、不确定可信威胁多等挑战。由此,他们围绕车联网软件“端-云-网”特征,以终端软件、网络通信软件、服务端软件可信技术研究为切入点,建立了一套完备的客户端软件设计与开发、验证、动态部署以及实时控制相关可靠性保障技术体系;实现了资源受限下移动网络的可靠数据传输与认证,以及异构网络融合技术;通过软件执行环境实现对服务端软件可信保障核心要素进行筛选,集成和验证了基于虚拟化的网络软件实体可信保障机制,以及基于监控的可信追溯机制和相关的可信保障关键技术。

在此基础上,研究人员研制了车联网软件可信技术综合集成验证平台,通过接入实际车辆以及对接仿真数据生成平台,对可信保障机制进行综合试验与验证。同时,针对车辆监管、专车服务和Telematics服务等不同典型场景,研究人员搭建了面向车联网的大数据云服务平台和信息服务平台,实现车接入超过7万辆,成为世界上规模最大的车实时数据处理平台系统之一。

据了解,相关技术和成果已经应用于交通部重点营运车辆监管系统,北京市、重庆市等地方交通管理机关实时交通业务系统以及新型交通运输企业移动网联平台,社会效益和经济效益明显。

研究人员表示,在提高车联网等软件的可信度之外,相关技术和成果也为后续发展提供了可信技术支撑,为提升信息化带动工业化能力、落实网络环境下工业控制系统安全和可信提供了基本技术手段和试验验证环境。

### 1 看准趋势 从“能不能”到“信不信”

2018年8月中旬,刚入秋北京清晨已有些许凉意,中关村附近的一个菜市场内人群熙攘。挑选好一样蔬菜后,张大爷拿出兜里的智能手机,熟练地通过扫小摊上挂出的蓝色二维码支付了菜钱。和十多年前网上支付刚刚启动时的情况不同,今天,即使上了年纪的大爷大妈们,也不会因为担心手机支付不安全,而拒绝使用支付宝、扫码支付。

人们对支付软件的信任,来源于软件本身的“可信性”,意指软件系统是否能在操作错误、环境影响、外部攻击等干扰下,依然提供连续的预期服务。

如今,以通信、存储和计算为核心的信息基础设施已经渗透到人类生活的方方面面,软件对“可信性”的要求,显然不限于网络支付领域。

早在十多年前,中国计算机科学家已经注意到,随着软件的应用需求越来越多,复杂度越来越高,可用性要求越来越强,软件系统也越来越庞大,越来越脆弱。“软件不总是可以让人信任的,很多时候它并不以人们所期望的方式工作,会发生各种故障和失效,从而直接或间接地对用户造成巨大损害。”中科院院士、华东师范大学计算机科学与软件工程学院教授何积丰表示。

1996年6月4日,欧洲阿丽亚娜5型火箭在首次发射中由于惯性参考系统软件的数据转换错误导致软件失效,发射40秒后爆炸,造成25亿美元的经济损失。2005年11月1日,日本东京证券交易所由于软件升级出现系统故障,导致股市停摆。2007年北京机场信息系统瘫痪,至少造成84个航班延误。

在2017年12月举行的国家自然科学基金委员会(以下简称基金委)可信软件基础研究重大研究计划(以下简称重大研究计划)结束评估会上,作为指导专家组组长的何积丰在报告中提及上述案例时,与会专家依然对过去种种因软件可信性导致的损失感到万分惋惜。

时间回溯到2007年底,面对当时由于网络交互、共享、协同等带来的“不可信”因素,基金委在广泛听取各界专家意见和反复深入研讨的基础上,由信息科学部、数学物理科学部和管理科学部联合组织,及时启动了该重大研究计划。

用何积丰的话说,这是“我国软件基础研究领域的一件大事”。“我们对软件关注的重心从‘能不能’转向了‘信不信’。”何积丰告诉《中国科学报》记者。

此后,国家层面相继启动了“863”计划、“十二五”规划等,支持相关领域的研究和发展。在业内专家看来,正是该重大研究计划的启动及基础研究成果引领了国内这一领域的发展。

### 2 需求导向 直指“卡脖子”问题

围绕可信软件面临的机遇和挑战,科学家们将主攻问题锁定在国家关键应用领域,并按“以重点领域应用需求为导向引领理论和技术研究,以理论和技术研究成果支撑综合试验平台的研制,以综合试验平台承载典型应用示范”的路线实施该重大研究计划。

2010年至2013年,科学家们在陆续完成可信软件理论体系和技术体系的积累后,将研究成果在各类试验环境中进行示范,真正让可信软件技术走出实验室,走进国民经济主战场。

本文开篇的场景中,人们对网络支付的信任,得益于该重大研究计划中建立的我国首个互联网交易风险防控体系。这一体系已服务21个国家和地区,4亿多支付宝实名用户。该重大研究计划科学家、同济大学计算机系教授蒋昌俊介绍,该研究从运用到实践3年来为支付宝减少财产损失173.03亿元,资金损失率仅为万分之零九,是发达国家同领域资金损失率的两百分之一。

此外,还有1000多万行代码应用在我国探月工程、载人航天、北斗导航等型号的各类航天嵌

式软件中,打破国外技术垄断的列车通信控制器,3年为支付宝减少170余亿元损失的首个互联网交易风险防控体系,连续4年没有发生重大事故的电子税务可信监控,实车接入超过7万辆、世界上规模最大的实车实时数据处理平台系统……据统计,该重大研究计划在重大示范应用方面共完成项目15项,与长城华冠、中航工业615所、航天五院、全路通、核九院、支付宝等机构开展合作,推动国家安全相关行业自主可控技术发展。

谈到收获与感想,该重大研究计划科学家、中国空间技术研究院杨孟飞院士表示:“重大研究计划的实施过程中,我们边研究、边验证、边应用,软件质量显著提高,研制效率显著提升,逐步实现了从局部到系统、从依赖人到依赖工具的转变。”杨孟飞院士介绍,“集成项目实施以来,软件交付的缺陷率显著下降,百余个航天器在轨运行未发生软件质量问题。”

在科学家们看来,以需求为导向开展基础研究,切实解决了诸多领域中的“卡脖子”问题,有力支撑了国家战略。

### 3 完善体系 引领该领域由弱到强

在重大应用示范取得成功的背后,离不开基础理论研究和技术创新平台的突破。该重大研究计划启动之初,指导专家便对长达十年的科学研究绘制了蓝图,不仅提出了科学目标,研究内容要点和核心科学问题,还精心对目标进行分解,制订了进度计划。

十年里,科学家们围绕“软件可信性度量与建模”“可信软件的构造与验证”“可信软件的演化与控制”和“可信环境的构造与评估”等四个核心科学问题取得了丰硕成果。

“共发表2641篇论文,其中SCI检索803篇,EI检索1495篇;国家级科技奖励共计12项,省部级奖励31项。”何积丰用数据勾勒出该重大研究计划取得成果的概况。

这些数据反映的是,我国可信软件基础理论研究实现了跨越式发展。例如,可信软件理论与方法元级框架的提出,实现了从传统正确性向开放、动态、多变环境下的软件可信性跨越;标准化科学化的可信计算环境构造与评估体系的建立,实现了从部分环节可信计算向全栈可信计算跨越;软件过程和制品的可信性度量体系的建立,实现了从分散的可信度量向系统化度量跨越;网络软件监控与演化的一体化设计体系的提出,实现了从静态补丁式演化向动态模型驱动体系结构的跨越。

同时,基础研究的跨越发展牵引带动了技

术平台实现创新性突破,多项关键技术集成,为软件全生命周期工具集的设计奠定了技术基础。例如,提出了基于基准测试的代码级可信保障工具评价方法,研制了一批自主软件工具,建立了基于虚拟架构的可信云计算支撑环境。

2016年,英国皇家工程院院士、英国伦敦大学教授彼得·奥赫阅读中国学者在计算机领域顶级会议“计算机辅助验证”(CAV)发表的论文后,高度评价称:“这正是我所渴望的工作。”

十年来,一支以中青年人才为主的高水平研究队伍,一批站在世界科学研究前沿的学科带头人,也在该重大研究计划实施过程中成长起来。来自我国70多家单位的1000多名计算机领域的学者合力攻关,共同推动我国可信软件实现从小到大的跨越式发展,进入该研究领域国际先进行列。

面向未来,何积丰表示:“为巩固和辐射本重大研究计划的成果,应及时建设可信软件开发资源与服务平台,充分利用群体智慧,建立形成可信软件的开放数据、开放服务、让合作开发成为可能。”

同时,科学家们也期待,在可信软件与人工智能交叉的新领域有所作为,以满足我国工业4.0和机器人等国家创新计划对可信智能化软件不断增长的迫切需求。

## 确保载人航天顺利开展

■本报见习记者 辛雨 记者 甘晓

随着我国航天事业的快速发展,空间站、探月工程、高分专项等一批复杂航天任务陆续实施,软件在航天器中的作用和地位越来越突出,软件可信性已成为确保型号任务成功的重要因素。

目前,航天嵌入式软件可信性保障尚未形成系统解决方案,软件质量受人的能力、经验影响较大,导致一些深层次问题时有发生。中国科学院院士、嫦娥五号探测器系统总设计师杨孟飞带领研究团队,在国家自然科学基金委重大研究计划“可信软件基础研究”的支持下,以该重大研究计划相关研究成果为基础,针对航天嵌入式软件的特点,结合已发生问题的分析,建立了一系列可信保障工具,并构造了一个覆盖从软件需求分析、设计、编码、测试、编译固化到运行维护全过程的航天嵌入式软件可信性保障集成环境(SpaceDep)。

在专家们看来,这项工作实现了软件可信性保障从局部到系统、从依赖人到依靠工具的转变,提高了航天嵌入式软件的可信性。这些成果已经在百余个航天型号



“航天嵌入式软件可信性保障集成环境与示范验证与应用”集成项目启动

中得到验证和应用。

据研究团队成员、航天五院502所研究员顾斌介绍,该项目实施以来,软件交付的缺陷率显著下降,百余个航天器在轨运行未发生软件质量问题。

“近期,我国天舟一号任务成功实施,北斗三号任务也离不开在该研究中取得的成果。”顾斌说。

此外,相关研究成果还推广应用到国民经济的其他领域,创造了超过1000万元的经济效益。