

专题栏目策划人



杨义先

北京邮电大学教授、博士生导师、信息安全中心主任,灾备技术国家工程实验室主任,首批长江学者特聘教授,首届国家杰出青年基金获得者,中国密码学会副理事长;目前研究方向为网络空间安全、现代密码学和纠错编码等;获得包括国家发明奖和省部级科技进步奖等在内的各类科技奖励20余项,主持和参与多项国家“863”计划项目、国家自然科学基金项目、省部级等科研项目;发表高水平论文500余篇,出版专著及教材20多部,持有发明专利4项。



杨庚

南京邮电大学研究生院常务副院长,中国计算机学会、中国通信学会高级会员,教育部高等学校信息安全专业教学指导委员会委员、《计算机通信与网络》国家精品课程负责人和国家级精品视频共享课负责人;目前研究方向为云计算与大数据安全、信息与网络安全、分布与并行计算等;曾获省部级科技进步奖2项,主持和参与国家“973”项目课题、国家“863”计划项目、国家自然科学基金项目等8项,主持省级科研项目10项;近年来发表论文近百篇,持有中国发明专利20余项,已转让4项。

专家论坛栏目策划人



李军

清华大学信息技术研究院院长,清华信息科学与技术国家实验室常务副主任,中国电子学会计算机工程与应用分会副主任,工信部电子科技委委员;目前研究方向为网络信息分类与过滤、网络流量观测与控制、数据中心网络虚拟化等算法和系统方面的研究;作为“863”目标导向课题“一体化网络数据深度安全检测与分析的技术与系统”项目负责人,获得2014年中国电子学会科学技术奖二等奖;著译中外教材3部,发表学术论文百余篇,持有美国专利2项,中国发明专利15项。

专题:网络空间安全

专题导读

2015年,对中国信息安全教研界来说,最大的新闻莫过于“网络空间安全”被国务院学位委员会正式批准为国家一级学科。从此,高校的“网络空间安全学院”将如雨后春笋般大量出现,信息安全高级人才的培养将走上快车道。在这一关键时刻,如果没有做好网络空间安全体系的设计,积极探索网络空间安全的关键技术,那么很有可能会事倍功半。本专题的目的之一,就是希望借助《中兴通讯技术》,促进中国网络空间安全界尽可能多的同仁们形成合力,争取事半功倍!

网络空间安全是一个系统工程,必须重视顶层设计,必须从体系架构方面给予全面考虑。《网络空间安全面临的挑战及应对策略》和《网络空间安全体系及关键技术》两篇文章,在分析了中国网络空间安全现状及其面临的威胁后,探讨了应对策略;并通过分析传统线性结构防御体系以及传统的网络空间安全问题,提出了新型立体式网络空间安全体系结构,指明了网络空间安全技术的发展趋势和未来的研究方向。

“大数据安全”是网络空间安全的难点和重点,也是未来的热点。《云时代下的大数据安全技术和《面向数据的安全体系结构初步研究》两篇文章,分别从不同的角度,研究了大数据面临的威胁与挑战,从大数据安全体系、Hadoop安全架构、数据所有权确立、数据注册、防范APT攻击技术等方面提出解决方案,同时也提出了以数据为核心和面向数据的信息安全解决方案,即面向数据的安全体系结构(DOSA)。

云计算、大数据、物联网是“互联网+”时代关键的技术,然而如果没有安全计算,势必会严重影响它的发展。《安全多方计算技术研究与应用》一文,从介绍安全多方计算的概念开始,基于同态密码、格理论密码设计了实用的安全多方计算协议,并总结展望了安全多方计算协议研究发展趋势。

网络空间的命脉是安全,安全的核心是密码,而同态加密又是密码研究的最新热点。《同态加密的发展及应用》一文,综述了同态加密方案的发展,介绍了同态加密在安全多方计算、密文检索、安全云计算、电子选举等诸多方面的应用。还着重分析了一些部分同态、浅同态和全同态加密方案的优缺点,介绍了同态加密中存在的一些公开问题。

在数字时代,人们的生活越来越依赖于各种数据,“好事”和“坏事”都会在数字空间中进行,因此,“数字取证”就成为了网络空间安全的一个重要方面。数字取证也可称为计算机法医学,它是指把数字空间看做犯罪现场,运用先进的辨析技术,对电脑犯罪行为进行法医式的解剖,搜寻确认罪犯及其犯罪证据,并据此提起诉讼。《计算机网络取证和调查的科学研究》一文,通过一个真实的网络犯罪案例的犯罪现场重建,阐述了调查取证基本原则。并在此基础上,通过理论和实验分析,将取证科学过程应用到对P2P网络中某些文件的首次上传者调查中。

这期专题主要和大家一起来讨论网络空间的关键、热门技术。这些论文凝聚了作者多年的研究成果和工作经验,希望能给读者有益的启示与参考。在此,对各位作者的积极支持和辛勤工作表示衷心的感谢!

杨义先 杨庚

2015年12月21日