国家网络安全宣传周 China Cybersecurity Week

2018年国家网络安全宣传周 上海地区活动

全民共筑网络安全“防火墙”

网络信息人人共享，网络安全人人有责。2018年国家网络安全宣传周上海地区活动中，网络安全高峰论坛七个分论坛于9月18日到19日在上海复旦学术国际交流中心等地举行，主题分别为互联网创新技术与云安全、区块链应用发展与安全、金融科技风险防范与安全保障、网络安全治理与产业创新发展、智慧校园时代的高校网络安全建设管理、企业安全管理与文化、移动互联网应用安全。

■奚宇轩 成佳佳

区块链技术如何守护网络安全？

随着区块链技术的大热，不少人认为区块链将是未来网络安全领域对抗黑客、消灭安全漏洞等问题的最佳选择。在9月18日举办的“网络安全宣传周——区块链应用发展与安全分论坛”上，多名企业专家聚集杨浦，分享区块链的技术安全及应用场景。

全球交易量第二大的虚拟货币交易所遭受黑客攻击；雅虎数十亿用户信息遭到泄露；DNS域名服务器遭受大规模DDoS攻击……这些网络安全问题曾频频爆发。全新的区块链技术如何守护网络安全？

“目前，上海市信息安全测评认证中心已梳理出区块链风险20类左右，其中6类为新风险，其余为传统风险。这6类新风险包括整数溢出、短地址攻击、算力控制、双重支付、代码重入、恶意操纵节点。”上海市信息安全测评认证中心高级工程师徐御指出，区块链技术安全标准将采用开放架构设计、按照适度保护原则进行设计。针对上述安全风险，该中心已梳理了相应安全措施。未来或可从区块链产品信息安全认证和区块链项目安全评测两方面结合来定义一款区块链应用是否安全。

区块链技术具有可靠的信息交互、完整的数据存储、可信的节点认证等安全性优势，因而为网络安全提供了一种崭新的安全防护思路和模式，将传统网络边界式防护转变为全网络节点参与的安全防护新模式，通过分布式的节点共识机制来抵抗恶意节点的攻击，在网络安全领域具有极大的应用潜力。

现阶段技术还不够成熟，区块链系统仍然存在安全隐患和漏洞。近年来，上海着力推动区块链底层技术的研发和应用落地，已汇聚100余家区块链技术企业及科研机构，底层技术研发实力已处于全国领先地位。作为全国首批大众创业万众创新示范基地，杨浦也在积极布局区块链产业。今年6月，国内首个省级区块链技术研究中心在同济大学成立，致力于汇集顶尖区块链技术研发人才，加快区块链领域的自主核心技术研发与应用，充分发挥其安全优势，有效提升网络安全防护水平。

很多人对区块链的印象还停留在早先比特币病毒勒索案件。但实际上，虚拟货币只是区块链技术应用的一个场景，如今区块链技术已从金融行业延伸至电子商务、智慧医疗、社会保障、物联网等多个领域。区块链的发展前景广阔，但目前实际落地仍然受限，怎样将其更好地应用到具体场景中去？

“什么是点对点？用微信、支付宝扫一扫能看到出现的二维码，这就是点对点的体现。”爱迪实验室创始合伙人胡冬解释说，区块链技术在金融领域已有立足之地，支付宝利用区块链技术做到了“一秒到账”，解决了传统技术信息不同步的问题，极大优化了用户体验。

胡东表示，即将到来的区块链3.0时代是价值交易的云服务平台，是超出金融领域，为各种行业提供去中心化解决方案。区块链的应用领域扩展至金融行业之外，覆盖人类社会生活的方方面面，在各类社会活动中实现信息的自证明，不再依靠第三方或某机构获得信任或建立信用，实现信息共享，包括在司法、医疗、物流等领域，区块链技术可解决信任问题，提高整个系统的运转效率。

区块链未来发展的产业方向可以是公共服务、共享经济、金融创新和供应链管理等领域。如，阿里健康运用区块链技术把医疗信息上链，健康中心和地区医院互联互通，不仅节约成本，而且让市民享受到更便利、安全的医疗服务。

联防联控形成金融安全生态圈

金融科技在快速发展过程中面临着不少问题和风险，对传统金融监管提出了全新挑战，如何保障金融安全？在9月19日举行的“2018国家网络安全宣传周上海地区活动——金融科技风险防范与安全保障分论坛”现场，多位专家学者就金融科技安全问题开展了热烈讨论。

“2016年孟加拉中央银行在美国纽约联邦储蓄银行开设的账户遭遇不法分子攻击，失窃8100万美元。同年7月，不法分子攻击台湾某银行自助渠道系统，远程控制ATM机自动吐钞，在60个小时内取走了7000万台币现金，平均每五分钟就完成一次取现操作……”中国建设银行上海分行金融科技部副总经理李准一上台就列举了多起针对金融行业的网络攻击案例。以盗取资金为目的的常规攻击不断演变，恶意链接、病毒木马等供给手段层出不穷。

针对金融科技遇到的上述安全挑战，李准表示，企业要以电子渠道交易风险和客户敏感信息泄露风险为切入点，建设灵活可配置的安全服务，动态规划防控规则，全面支撑未来业务创新和快速发展需要，减少新型业务产品安全风险，保障资金交易安全和客户新型资产安全。他还提到，银行可与公安机关、运营商、第三方机构等不同层次外部机构共享威胁情报数据，挖掘客户资金损失和信息泄露方面的风险，联防联控共同处置风险事件，形成金融安全生态圈，从而达到全方位保护客户资金和信息安全的目的。

“目前P2P行业累计的问题企业数量已占行业总量的三分之二以上，健康存活率不足三分之一。整个新金融行业的高风险性可见一斑。”上海数荃数据科技有限公司首席技术官马海兵给出一个数据，截至9月14日，整个P2P行业累计的问题企业数量达4664家，而整个行业才6560家企业。他认为，从新金融风险产生的原因来看，首先，有闲散资金并希望获得高收益回报的小散户本身承受风险能力较弱，且容易产生挤兑现象，涉及的又是风险相对较高的金融业务，因此新金融行业本身就存在高风险。其次，互联网金融的运营模式由于违规成本较低，容易让不法分子铤而走险，用于非法集资。

监管部门应如何协调各方利益，处理好监管和创新的关系，如何破解“一放就死”的难题？

“目前新金融监管存在的问题主要有信息匮乏、利益冲突、对象不明、手段单一、人员短缺、监管缺失等。”马海兵指出，对新金融行业而言，适时、及时、科学、适当的监管非常必要，他建议应用大数据手段创新监管方式。“我们希望建设一个新金融的监管平台作为枢纽，将监管方、金融机构、从业者、社会四方融合到一起，构建一个四位一体的监管体系。”

据悉，上海数荃数据科技有限公司成立于2016年，是上海大数据产业联盟发起单位、上海市信用数据交易平台建设单位，同时也是贵阳大数据交易所副理事长单位。同年11月，杨浦区金融办与上海数荃数据科技有限公司签约，共建“新金融风险综合监测服务平台”。该平台正是基于大数据技术，提供针对新金融行业的数据采集、建模分析、分业监测、量化评估、风险预警等全流程处理，提供灵活快捷的信息查询和分析研报功能，提升区域金融维稳水平。

杨浦区政务外网光缆预警系统发布

在网络安全治理课题中，如何运用最新的信息安全领域攻防技术，对政务安全、网络安全和关键信息通信设施安全，提供技术保障和完整解决方案？9月19日，“2018年国家网络安全宣传周上海地区活动——网络安全治理和产业创新发展分论坛”举行，“大咖”们就网络安全治理方案展开热议。

复旦大学光纤研究中心主任、国家科技部重大专项负责人贾波教授，作了《光纤通信传输安全面临的挑战和对策》的主题报告。“光缆所处的环境比较复杂，地埋光缆铺设上千公里，这意味着它受攻击的可能性非常大。”贾波指出，光纤安全会带来诸如信息窃取、信息篡改等一系列信息安全隐患。而如今光缆被无意识挖断、光缆被“非法窃听”（棱镜门事件）、光攻击导致系统瘫痪、干扰通信等都是常见的攻击形式。

针对当前网络空间存在的各种威胁，和当前国际信息安全技术发展现状，贾波提出利用自主知识产权的核心产品，实现全天候威胁感知技术，以确保通信安全的发展理念。“光缆安全预警技术是切实可行的光传输安全保障技术，能够做到事故前预警，并为光缆提供完整的地标信息，现在城市里光缆断了，需耗费四五个小时才能完成事故勘查，而通过该技术30分钟内即可完成。”

论坛上，复旦大学与杨浦区科委联合推动的杨浦区政务外网光缆预警系统发布，并进行了现场演示。据了解，该技术针对光缆这一当前我国最广泛的关键信息基础设施面临的风险，能准确、及时地识别外部挖掘损毁等破坏行为，信息窃取、篡改和非法加载等威胁行为，并进行定位，发出预警，从而为包括政务网、专用网络、金融关键通信线路、国防通信线路提供智能安全保障。杨浦区科委负责人表示，这是响应国家号召，加快构建关键信息基础设施安全保障体系的具体举措。

现场，区科委与复旦光纤研究中心举行合作签约仪式，双方约定，将共同推进复旦大学的技术转化，为高校创新技术服务地方，进而为上海打造国际创新中心贡献力量。记者了解到，未来，围绕下一步校地合作，杨浦将与复旦大学开展信息安全技术在政务安全领域的全面合作。