

杨珉获首届“上海市网络安全工作特殊贡献个人” 放弃公开发表成果,他汇报了研究进展

“在网络安全研究中发现问题时,相比起发表有影响力的论文,国家利益的损失与否是我最先考虑的,这也是我们团队的价值观。”杨珉说。

我校杨珉教授近日获“上海市网络安全工作特殊贡献个人”荣誉称号,表彰杨珉团队为上海市网络安全工作做出的重大贡献。该奖项是2014年上海市委网信办成立以来首次颁布的奖项。

长期聚焦于安全攻防技术研究,近年来围绕AI安全研究的杨珉团队,提出基于安全攻防视角的智能系统模型安全测评理论与方法,揭示了多领域AI模型安全缺陷的机理,实证了人工智能技术大规模应用于开放网络环境时存在诸多重大安全隐患。

此次获奖,正是杨珉团队发现了身份认证机制存在的重大安全问题,直接影响了众多平台,导致国民大数据面临严重的大规模泄露风险。立足国家利益和国家安全,杨珉团队放弃公开发表研究成果,第一时间向有关部门汇报研究进展,并协助向涉及平台提供相应的安全防护措施与技术手段,避免了重大安全事件。

“我们就是做了这样的一件事”,杨珉说,“虽然表彰的是我个人,但实际上是对我们团队在安全研究方面的肯定。”

在发现与研判问题后,杨珉第一时间向学校上报情况,并在学校统一部署下,配合有关部门开展一系列后续行动。对此,杨珉表示:“在信息安全这个核心问题上,国家利益无条件优先。”

安全研究领域的护航人

“做安全研究,我觉得是我的使命,也是浪漫的一件事。”

2007年杨珉博士毕业后,留校开展操作系统和编译工具链的研究,2011年在计算机系统最顶尖的国际学术会议 Usenix ATC 发表了来自中国大陆的第一篇论文。但他觉得还不够,2010年,他前瞻性地做了一次重大的转型选择,开始在安卓平台上做安全研究。

为什么转型到安全研究?杨珉说:“每个人都希望做点不平凡的事,那怎么去选择?选择的方向在哪里?需要能代表未来,必须是国家的重大需求,必须有足够高的研究门槛。安全很重要,但以前一直是附属品的角色。随着信息技术与现实世界的高度融合,尤其是以移动数字生活为代表的形态展示了无以伦比的发展速度,网络安全会成为必需品。我意识到,安全问题是更感兴趣同时又非常重要的一个领域,所以逐渐的就从这些基础软件领域转移到网络与系统安全领域的研究。”而操作系统和编译技术领域的扎实基础奠定了他的技术功底。

经年累月的研究下,杨珉团队将技术跨度很大的软件安全评测技术与人工智能技术融合在一起,形成了独具一格的面向智能系统安全分析与增强理论与技术体系,在整个行业中也极具创新性。并且,这个技术具有很强的普适性,可以服务不同业务场景的安全需求。“我们团队的技术,除了服务于移动软件的

安全检测,譬如各种app、小程序等,在网络关键基础设施、互联网企业、金融、智能网联汽车等各种平台系统中也能有所作为。它可以用来发现各种系统软件中存在的未知安全漏洞,构建新型的安全体系结构,提升这些系统的抗攻击能力。”

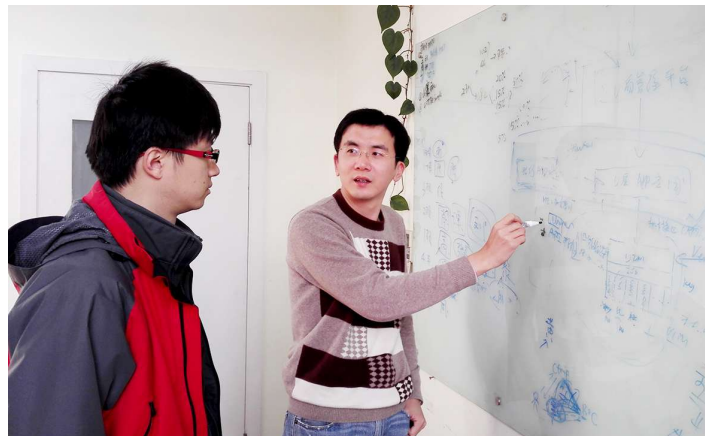
聚焦国家战略亟需,杨珉如今已成为网络安全领域的领军人物。2020年计算机领域国际权威排名 CS Rankings 显示杨珉所在的计算机学院网络安全方向全球排名第八(国内排名第一),团队孵化的复旦白泽战队多次荣获国内外顶尖安全攻防竞赛冠军,为行业输送了一批高水平人才。

网络安全是一个比较特殊的领域。“如果没有良好的价值观、道德情操和法律意识,很容易走歪,造成严重的社会危害。”因而,在培养学生时,他时刻强调家国情怀,更加注重培养学生的价值观。

网络安全技术是一把双刃剑,“如果能率先发现漏洞,可以及时帮助我们国家的重要系统打上补丁、应对攻击。同时,如果我们能发现对手侧的问题,那在国家间的博弈当中,它又是一个武器。”杨珉说,在安全领域深耕,是时代赋予他的使命。

“我们还需要做很多事情”

在我国的信息化进程当中,很多网络安全的思想、技术到管理机制,曾仿照欧美成熟的经验和模式。但是,随着发展与进步,在不少信息技术细分领域中,我们已经逐步走到国际前沿,尤其是在移动互联网的业务场景中,



■ 杨珉带领团队充分发挥复旦文理融合的学科优势,在服务国家、科学研究和人才培养等方面取得一系列进展,研究成果多次获党和国家领导人重要批示并为相关部委采用。

中国的很多应用已经走出了自己新的商业模式和应用模式。“人工智能的各种技术被广泛应用于开放环境中,这种实践欧美国家已经滞后,我们在移动互联网上出现了很多赶超和创新。但同时也意味着我们失去了仿效的对象。”杨珉说。

信息化技术的发展日新月异,但是在新技术发展过程中,也伴随出现了大量新型的、未知的安全问题。“这就要求,安全检测和评估技术需要同步发展,但事实上安全检测评估技术,包括安全防护技术,都比较滞后于新型信息技术的发展。”

加强网络空间的安全,还有很多路要走。而这其中,技术不是唯一选项。

杨珉说,网络安全问题的严峻性首先应该得到思想上的高度认知。从2017年网络安全法实施到今年数据安全法、个人信息保护法的实施,国家层面上一直都

在明确网络安全的重要性。“当前大国博弈非常激烈,尤其是网络安全技术在2013年就成为西方国家对华禁运的门类,这必须得靠我们中国科技工作者进行自主创新和突破。”

“在互联网的发展和国家治理数字化转型的大背景下,发展和安全需要统筹考虑。高水平人才的培养,是大学一个核心的使命。从人才培养体系、科研范式到课程体系等都面临着一些全新的挑战,需要进行突破,我们也正在努力着。”

“此外,我们需要重视新型信息化技术的规模化应用带来的安全风险。相关的安全风险评估评测工具需要不断迭代,去攻关、去破解这种卡脖子问题。”杨珉强调,网络安全是一个攻防博弈特别激烈的一个领域,“需要不断持续地去研究、演进和提升的一个基础领域,要做的还有很多。”
文/章佩林

附属儿科医院第二届行风征文获奖作品

附属儿科医院完成注射上海首例儿童法布雷特效药

“16岁,男孩,首次入院”。4年前——手指尖、足趾尖阵发性疼痛、前胸及后背散在红色皮疹;1年前——眼睑浮肿、蛋白尿;6月前——肾功能异常、脾肿大、心肌肥厚”。

这是接诊医生在问诊小宇妈妈后记下的对小宇病情的第一印象,她眉头紧锁的同时不禁心中一沉,意识到这不是一位普通的肾脏病患儿。

同样眉头紧锁和忧心忡忡的还有男孩和他的母亲,从溧阳,辗转南京,再到上海,求医的艰辛和曲折已被5cm厚的病史资料描绘得淋漓尽致。然而,妈妈的又一席话更是震惊了这位医生——“他姥爷36岁就去世了,舅姥爷53岁也去世了,我也身体

不好有肾炎,哎,我们家真是造了什么孽哦……”

小宇罹患的到底是什么毛病?神经、皮肤、肾脏、脾脏、心脏似乎都有问题,过去的治疗也是“头痛医头、脚痛医脚”,说不出个所以然来。

“哦,这里还有几个报告,刚拿到,南京医生说特别重要……”小宇妈妈又小心翼翼地拿出了几张用薄膜袋包着的纸,尽管这几张纸仅仅几毫米厚,但是它们给接诊医生带来的冲击远超那5cm的“炸弹”:一份肾活检报告:肾小球弥漫增生硬化、大量髓样小体……

看到这些结果,接诊医生也楞了一下,Fabry病(法布雷病)?这是在书上才看到的名词。于

是他立即找了治疗组的上级医师寻求帮助。

法布雷病是一种罕见的X染色体伴性遗传溶酶体贮积病,目前存在以下的诊治困境:临床医生认识不足;初发症状特异性不高,临床表现多样,可累及多个系统;延误诊断率高等。据报道,法布雷病成人患者从首发症状到确诊平均延误15年,儿童患者约4年;部分患者诊断延误可达30年或更长时间。

在充分了解小宇的病情后,治疗组喜忧参半。喜的是,他在16岁这年明确了诊断,目前已有特异性酶替代治疗药物被批准用于该病的治疗,使得法布雷病成为为数不多的可诊可治的罕见病之一;忧的是,治疗的费用

昂贵。

医生办公室的气氛冷了下来,被安置在加床上的小宇坐在床沿,无序地翻动着手中的课本,他的妈妈也沉默地坐在一边,手指搅动着衣角。这个梦想考上第一梯队大学的孩子,是否可以在象牙塔继续追寻心中的梦想……

这个不服输的家庭选择了坚持治疗,但要面对现实,光靠信念并不能救治。法布雷病的“筛查”、“诊断”、“治疗”、“随访”是圆环的四个弧度,缺少哪一个,都不能“圆满”。而这,需要多学科团队和社会团体的共同参与。

为此,徐虹教授作为专家协作组成员参与了2013年中国法布雷病专家共识的撰写和推动

工作,牵头集聚肾脏科、神经科、新生儿科、皮肤科、风湿科、分子诊断中心科等十余个相关科室力量,率先在国内成立了首个儿童法布雷病MDT团队;并与全球单中心最大组法布雷病诊治中心(瑞金医院)陈楠教授合作,对确诊成年患者的子女进行综合评估并制定个体化治疗方案;在社发部的支持和推动下,成立“清新之爱-儿童法布雷病紧急救助专项基金”慈善项目。

他们是法布雷患儿,他们是罕见病群体;每一个小群体都不应该被放弃,这也是中国力量!

在多方的努力下,上海首例儿童法布雷特效药(注射用阿加糖酶 β)在附属儿科医院完成注射,小宇就是这位幸运儿。

阳光依旧洒在课本上,这次折射出的是金灿灿的希望……

文/张致庆