

新软件识别偷玩手机的“熊孩子”

今日头条

本报记者 江耘

如今,越来越多的未成年人变成了“手机控”,沉迷手机无法自拔。不少孩子因过度使用电子产品而引发视力下降、骨骼发育不良等疾病,甚至出现自制能力下降、心浮气躁等心理问题。

统计显示,大部分3到12岁的孩子每天会花1到3小时的时间接触手机等电子产品,13到18岁的青少年每天花在手机上的时间甚至可达3到6小时以上。如何才能让孩子远离手机呢?

机呢?

近日,“国家青年千人计划”入选者、浙江大学电气工程学院智能系统安全实验室徐文渊教授团队和美国南卡罗来纳大学合作,开发出一种基于行为识别的算法软件。该软件能通过识别操作者的手势等细节,判定出当前使用手机的是成年人还是小朋友。未来,这款软件有望能通过各种方式限制未成年人的手机使用行为。

实际上,目前市场上也有很多能管理并限制手机使用行为的软件,但它们为何无法根治手机沉迷问题呢?

徐文渊告诉科技日报记者,这些软件多采用被动防范的方式,即在使用前需要打开软件进行设置,之后软件才能起到限制作用。如果没有启动该软件,孩子还是能玩手机,起不到控制作用。

相比之下,徐文渊团队开发的软件更强调主动防范。徐文渊表示,团队通过获取手指按压的面积、施加的压力、滑动的长度等度量数据,从而判定使用者是否是未成年人。如果是未成年人就会启动主动限制功能,这样就不怕“熊孩子”偷拿手机去玩了。

目前,这一软件识别的准确率已达97%,但依旧有3%的失误率。“若放到全国手机用户群体中,这个量也很庞大。”但徐文渊说,可以通过增加一些辅助手段来解决软件判断错误问题。

安装该软件后,软件如判定是孩子在使用手机,它会友好地提醒小朋友;若孩子偷偷用手机购买游戏装备,软件则会限制其交易行为。据悉,该技术尚处实验室研发阶段,还需后期不断完善。徐文渊表示,目前软件只是一种基础算法,并未被整合到手机的操作系统中。

在市场化应用方面,徐文渊希望有合作方加入,共同完成市场化开发工作,让技术转化为应用,让手机不再成为“熊孩子”的最爱。

IT辣评

点评人:本报记者 王小龙

快手急招内容审核员 算法时代内容还得人把关



因低俗内容被约谈并勒令整改后,短视频平台快手在清明节假期期间宣布紧急扩充审核员队伍,并已清理5.1万条问题短视频,封禁用户1.1万余人。此前,中央电视台《新闻直播间》等节目对快手、火山小视频等短视频平台上存在的未成年孕产妇现象做了报道。4月4日,国家广电总局约谈今日头条、快手相关负责人,要求其将网站上涉及低俗、暴力、血腥、色情等内容的节目立即下线。

点评:这一幕似曾相识,今年1月,在遭整顿后,今日头条也曾大规模招聘内容审核编辑岗位,加强内容审核。连岗位要求都极为相似——“有良好的政治觉悟与素养”“党员优先”。4月3日,快手CEO宿华在清华大学的一次活动中也进行了反思,他表示:“我们必须给算法加上我们自己的人文思考,我相信算法是有自己的价值观的,我们必须让算法实现和放大我们坚持的价值观。”在被约谈、被整改后,以技术为主导的互联网公司终于意识到,在算法主导时代更需要把关,更需要“总编辑”和审核员。

提前完成7纳米工艺开发 三星尝到了芯片的“甜头”



据外媒报道,三星电子已于近日利用远紫外光(EUV)设备完成了7纳米芯片工艺的开发。最初,这家韩国半导体巨头计划在年下半年完成这项技术,但最终提前6个月实现目标。三星的这项新技术将在今年投入量产,目前该公司正准备向高通提供样品。据悉,高通是三星7纳米工艺的首家企业客户。

点评:不但顺利完成了7纳米芯片工艺的开发,还提前了6个月。三星可谓是在芯片领域铆足了劲。之所以这么拼命地干,是因为三星尝到了芯片的“甜头”。三星对移动领域的长期关注与投入,尤其是在内存与芯片领域的投入,为其带来了丰厚的收入。在手机芯片领域,三星最大的对手是台积电。为了赶超对手,三星甚至已经启动了5纳米工艺的研发工作,并在韩国建造一座远紫外光芯片制造产线。提前布局、提前研发、提前完成,先声夺人也许是三星的一条制胜之道。

支付宝被央行罚款18万 以做效尤! 体量越大责任越大



日前,据中国人民银行杭州中心支行披露,支付宝(中国)网络技术有限公司因多项违规,被罚款18万元。支付宝方面回应称:“2017年下半年,我们在接受央行杭州中心支行的检查时发现了一些问题。我们第一时间启动了逐项的改进计划,目前各项改进措施已经落实完毕,并得到了监管部门的认可。感谢监管部门的指导和帮助,我们会在今后的工作中更加严格要求自己。”

点评:最近,有关隐私的问题成了大众关心的热点。支付宝的问题也与此相关。根据相关文件,支付宝的违规行为主要涉及客户权益、产品宣传和个人信息保护三大方面。作为一家拥有海量用户的互联网金融服务机构,支付宝的违规行为可能造成的社会危害不容小觑。罚是罚了,支付宝的态度看上去也算诚恳。但这么小的数额能否起到警示作用还有待观察。目前对这类超体量的互联网金融机构,在立法和监管上还存在一些漏洞,如何在发挥其社会价值的同时,约束并规范其行为将是一个新课题。



从IPv4到IPv6 安全要跟上技术升级的脚步

本报记者 付丽丽

近日,据媒体报道,有IT专家称发现了首例基于IPv6的分布式拒绝服务(DDoS)攻击,来自1900个IPv6地址背后的计算机设备向目标域名服务器发起进攻。

“这只是新一轮网络破坏活动的开始。”有互联网工程师如是警告。

当前,由于全球网络设备总量迅速攀升,现有基于IPv4协议的全球互联网面临网络地址消耗殆尽、服务质量难以保证等制约。IPv6能提供充足的网络地址和广阔的创新空间,这意味着有更多的设备可以接入互联网,因此业界对IPv6呼声颇高。

然而,正当全球各国积极部署IPv6之时,针对它的攻击也悄然而至。那么,IPv6存在哪些技术缺陷?我国又该如何将其补足?

击通常采用消耗网络带宽等方式,以求让目标信息系统无法正常提供服务。

而分布式拒绝服务是拒绝服务攻击的高级形式,它通常借助客户/服务器技术,将多台计算机联合起来形成多级攻击平台,实现对一个或多个目标的拒绝服务攻击,这种方式成倍提高了拒绝服务攻击的威力。

在分布式拒绝服务攻击中,大量计算机同时访问目标服务器,导致服务器的流量剧增,从而无法正常提供服务。

域名服务器是本次攻击的目标,它主要负责将域名转换成与之相对应的IP地址。闫怀志认为,此次网络专家发现的异常流量,就是指向域名服务器,意在摧毁其正常解析能力。

“这种攻击方式并非只针对IPv6,只不过是来自IPv6,指向IPv6而已。”闫怀志说。

的确,也有专家表示,此次攻击并未采用专门针对IPv6的攻击方法。但由于其来自IPv6并指向IPv6,引起安全人员的高度重视。

2012年就曾出现过类似攻击

偶然间,网络专家韦斯利·乔治注意到了一些奇怪的流量,这是针对一台域名服务器发动的大规模攻击的一部分,企图让服务器不堪重负。乔治供职于美国Neustar公司的SiteProtect DDoS保护服务部门,他当时正在收集恶意流量的数据包,并立即意识到“这些数据包源自IPv6地址并指向IPv6主机”。

此次事件,国内很多报道将其称为首例针对IPv6的“拒绝服务攻击”。

“其实这并不是首例拒绝服务攻击,更谈不上是首例基于IPv6的攻击了。”4月8日,北京理工大学软件安全研究所副所长闫怀志在接受科技日报记者采访时说。

闫怀志介绍,早在2012年2月,美国信息安全公司Arbor Networks就在年度研究报告中称:“出现了针对IPv6的DDoS攻击,这是攻击者和防御者之间‘军备竞赛’的一个重要里程碑,针对IPv6的DDoS攻击将会越来越常见。”当时,有4%的受访者就表示,他们曾见过IPv6网络遭到这类攻击。

对此,360安全专家李洪亮也表示,严格来说这不能算是基于IPv6的首例攻击,只是目前已知的基于IPv6的最大规模分布式拒绝服务攻击。“当然,随着IPv6的资源越来越多,攻击也会越来越多。”他说。

新协议也存在诸多隐患

“应当承认,IPv6协议与IPv4相比,在保密性、完整性、抗抵赖性、可认证性等安全性方面有了很大的改进。但从从来没有绝对的安全,IPv6协议也不例外,也存在诸多安全隐患。”闫怀志说。

具体来讲,首先,IPv6与IPv4的伴生和过渡所采用的双协议栈、隧道和地址转换等技术,给网络安全防护设置了更高难度。其次,IPv6协议为提升自身安全性而采取的安全机制,如被攻击者恶意利用,就会给安全识别和检测带来更大困难。

也有专家表示,多数IPv6网络存在于软件而非硬件中,这意味着其可能隐藏更多安全漏洞。另外,某些缓解工具仅适用于IPv4或仅提供IPv4版本,而后移植至IPv6。

如同互联网没有国界一样,网络空间的安全问题也没有国界,我国也不例外。

“国内的不法分子会针对IPv6网络发起攻击,国外敌对势力更会将矛头对准我国的IPv6网络。”闫怀志说,我国是最早开展IPv6应用的国家之一,也在一定程度上参与了国际IPv6标准的制订工作。

目前,我国正处于IPv6的大规模部署和应用阶段。因此,闫怀志建议,要从国家导向、安全意识、安全技术和安全管理等方面多管齐下,构建面向IPv6的网络空间安全保障体系。

“对我们来说,用IPv6的人越来越多,与之相匹配的设备也越来越多。IPv4环境下出现的安全攻击,也一定会出现在IPv6环境下。”李洪亮说,IPv6的大规模部署需要各方面努力,其中运营商应承担更多责任,最有效的方法是从事务角度引导用户和内容提供商迁移到IPv6环境下。

李洪亮认为,当前的安全防护设备、手段和体系等都集中在IPv4层面,尽管很多安全设备的入网许可需要通过IPv6测试,但在IPv6方面投入的精力还远远不够。他建议,以区域或行业为试点全面部署IPv6充分验证IPv6安全产品的成熟度。

DDoS攻击瞄准域名服务器

“从描述信息看,这是一次普通的流量型DDoS攻击,IP地址数量并不是很多。与其他流量型攻击不同的是,它发生在IPv6环境。”

闫怀志表示,拒绝服务攻击(DoS)是一种较为常见且危害巨大的攻击方式。这种攻击

区块链手机,是创新还是炒作

第二看台

本报记者 杨仑

在资本热捧下,区块链概念公司、产品层出不穷。一向精明的手机厂商自然不会放过这个机会。近日,连续多款声称具有区块链功能的智能手机密集发布,其中不乏老牌大厂联想和长虹。据报道,其他国产手机厂商也在酝酿推出相关产品。

区块链手机究竟是一款什么产品?它到底是创新还是炒作?

区块链标签纯属噱头

因“去中心化”的特色及“不可篡改”的特性,区块链被视为一种安全性极高的创新技术。但智能手机是如何与其联系到一起的?

今年已陆续有三家厂商发布了区块链手机,他们分别是:糖果的区块链创世版手机、

长虹的R8麒麟手机和联想的S5手机。三者对区块链的侧重各有不同,糖果手机与长虹手机宣称可以“挖矿”,联想区块链手机则主打支付安全。

“我认为,所谓的区块链手机纯粹是噱头。”知名科技自媒体人俞磊告诉科技日报记者,他已拿到了两款区块链手机,它们的共同特点是配置比较低,放在现在的市场环境中,“可能连水花都看不到”。

即便是在区块链技术上,这两款手机也乏善可陈。“倒是可以‘挖矿’,可挖出来的数字货币除了在商城里买点壁纸,几乎没有其他用处。技术上没有创新,应用上也未见得如何出色。如果这就叫区块链手机的话,那就把区块链看得太肤浅了。”俞磊说。

当前,区块链“挖矿”主要集中在PC端和服务端。捷孚凯市场咨询有限公司分析师金瑞兆指出,比特币是区块链技术的一个成功应用,但该技术对手机的价值尚在观察中。以手机芯片当前的运算能力来看,挖比特币一点可

能都没有。科技日报记者联系了多位手机业内人士,他们基本上都将区块链手机定义为炒作或噱头。

在集邦咨询分析师黄郁璇看来,区块链手机瞄准的是加密货币未来发展的可能性。“如果要区块链应用普及到日常生活中,智能手机的确有可能成为一个好媒介。”黄郁璇告诉记者,但在现有的技术环境下,区块链技术在应用层面上的创新还存在门槛。

蹭热点的背后是生存焦虑

区块链手机的推出时间,正值我国智能手机市场出现下滑之际。据统计,2017年全球智能手机出货量较上年下滑了0.5%,这是智能手机市场有史以来出现的首次滑坡。长期扮演智能手机市场助推器的中国市场,其出货量也出现了下滑。

智能手机同质化严重,新产品创新不足等因素延长了市场换机周期,这是导致销量下滑

的主要因素之一。在此背景下,大厂选择出海、市场下沉等手段维持自身利润,而规模较小的厂商只能依靠蹭热点来吸引眼球。

于是,厂商们在此时推出的区块链手机,是否真正在区块链应用层面实现了创新性突破,值得深思。

即将到来的5G时代更加剧了厂商的“求生”欲望。回顾历史不难发现,每一轮通信技术革命都会促成手机市场的洗牌。3G时代淘汰了诺基亚,4G时代小米等互联网手机企业迅速崛起。而在5G时代,国产手机第一梯队的优势正在持续放大,大量中小品牌或将被市场淘汰。创新性不足的产品可能面临巨大的生存压力,因此这些厂商追逐市场上的热点也就不足为奇了。

智能手机融合新技术本是一件好事,但需要的是真正的融合,而不是追求形式。无论是人工智能、5G,还是区块链技术,只有在使用场景、基础技术上取得突破,从而赋能智能手机,才能实现“1+1>2”的效果。

(本版图片来源于网络)

扫一扫 欢迎关注 畅游IT时空 微信公众号

