智能网呼唤“全链安防”

半夜收短信，银行卡被盗刷；传统企业网站服务器被恶意劫持，成了比特币挖矿机；自动驾驶成了四个轮子装个智能手机，会被黑客远程遥控……

随着人工智能、云计算、大数据、物联网等技术发展，安全问题日益凸显，面临从各种意想不到的维度影响用户安全的新挑战。日前，在以“安全强驱动，数字新生态”为主题的第四届互联网安全领袖峰会(CSS)上，与会专家和互联网安全业内人士，深入探讨未来的安全技术和防护对策。

技术升级换代 安全隐忧增加

今年以来，国内外连续发生多起网络安全事件。例如，某勒索病毒家族最新变种在国内爆发，一些政府机关、高校、医院等公共基础设施中招，导致众多文件和应用被病毒加密破坏无法打开。几个月前，国内一些医院服务器遭遇黑客入侵，攻击者暴力破解医院服务器的远程登录服务，利用某软件的分享文件功能下载多种挖矿木马以谋取利润。

加大数据保护力度、提升隐私保护能力也刻不容缓。据腾讯安全联合实验室发布的《CSS视角下的2018年全球网络安全十大议题》显示，目前数据及信息泄露事件频发，例如脸书(Facebook)5000万用户数据遭泄；新加坡遭最大规模网络攻击，黑客利用被恶意软件感染的计算机，窃取了150万新加坡人的健康记录数据。

与互联网等技术不断发展、传统领域数字化进程持续深入相伴随，安全问题变得越来越复杂，网络恶意攻击强度、频率、规模和影响在不断升级，安全“边界”将发生巨大变化。

中国互联网协会理事长邬贺铨院士说，5G时代将迎来网络能力开放的安全挑战。相比现有相对封闭的移动通信系统来说，5G网络如果在开放授权过程中出现信任问题，恶意第三方将通过获得的网络操控能力对网络发起攻击，规模将更大且更频繁。例如，5G应用在车联网，要求时延低至1毫秒，传统的认证和加密方式就不适用这种超高可靠低时延的通信场景。腾讯安全科恩实验室针对汽车企业提交的安全漏洞显示，恶意第三方可在非物理接触的条件下，实现远程控制车辆。

“这些新趋势和新问题，意味着安全不再仅仅是产业发展的能力补充，而是所有0前面的1。没有安全，所有技术创新都可能会失去意义。”腾讯高级副总裁丁珂认为，对企业来说，安全能力与新技术研发、应用同样重要；对行业来说，构建完善的数字安全新生态体系，才能有效保障并驱动数字经济的良性发展。

构建安全生态 打造防护网络

作为未来人们生活和工作的基础“能力”，人工智能安全尤其受到关注。

人工智能和其他的智能化技术一起，将把虚拟的数字世界和真实的物理世界紧密联结，数字世界中的安全问题都可能被放大为物理世界的安全事件。专家认为，无论是手机、空调、电视机，或是驾驶的汽车、飞行的飞机都可能被控制，造成物理性的损失。

每年以亿级数量增长的智能电视等智能设备，也成了被恶意攻击劫持的对象。比如一些具有在线购物功能的智能音箱，已成为黑客攻击和劫持的对象。人工智能设备和人的交互越来越频繁，便捷的同时也增加了攻击的可能性，人脸、指纹、虹膜等认证方式都成为攻击点。此外，人工智能为了给用户提供更好的服务，需要大量的数据来辅助，在数据采集、存储、流转过程中，都存在用户隐私泄露的巨大风险。

新技术不断进入日常生活，网络安全已不仅仅关系隐私、财产安全，还可能直接关联人身安全。丁珂认为，数字安全新生态的建设，需要以全新视角去理解安全问题，并跳出传统攻防概念，以协作为基础，推动政府、企业、用户联动，共同提升防护意识，避免链条中某一环节被攻破。

在今年年初腾讯安全玄武实验室首次发现的“应用克隆”攻击模型中，用户只要点击链接，攻击者即可克隆账户权限盗取账号和资金。这种“克隆病毒”就是基于一系列漏洞耦合在一起而产生的风险，并非某一个APP个案，而是移动APP面临的普遍问题。

不少专家认为，数字经济时代的安全已不再是单个企业或某个行业的事情，需要各机构、各领域协同合作，才能织好互联网安全的“防护网”，构建起整体安全防护。

(据《人民日报》)

手机应用“量”多更要“质”优

智能手机时代，每个人的移动终端里都有动辄几十个甚至上百个App，无论是苹果还是谷歌，都在各自的应用商店内为用户提供了海量的软件服务。各类App的“野蛮生长”，是对应用商城监管能力的严峻考验。

今年年初，工信部就曾约谈部分互联网公司，指出多款App对用户个人信息收集使用规则、使用目的告知不充分，涉嫌侵犯用户隐私。App“一触即开”，却也将潜在的安全隐患带给用户。有些App内容无聊低俗，安装时还会捆绑安装其他应用；有些App会在后台偷跑流量，甚至窃取用户隐私。移动互联时代，为用户提供内容丰富的选择固然重要，“量重质更重”的弦却一刻不能松。这需要多方合力，把用户的使用安全置于应用开发的核心位置。

首先，开发运营要严守底线。编程技术团队短时间内开发出一款吸金软件并非难事，加之上架渠道在安全监测方面设置的门槛极低，大量恶意软件才得以肆意上线。开发应用，原本应在合规合法的基础上满足用户的合理需求，若是偏离了最初航道，罔顾法律和道德大敛不义之财，就一定会被追究相应的法律责任。

其次，监管主体不能缺位。中国互联网协会法治工作委员会副秘书长胡钢认为，平台应从源头开始，加强全链条治理。上架平台对手机应用负有审核职责，相当于一个“把关人”，要把无益于用户甚至有害的内容挡在门外。有些应用商城平台封闭，理应承担起对App质量的监管责任，严格审核。而对相对开放的应用商城来说，更应加强预防，切实建立严格的应用审查机制。

最后，用户使用也得眸明心亮。陷阱多，就要求公众提高辨别能力，在正规应用商店选择App，尤其当软件内出现大额钱财的充值或消费时，更要提高警惕，避免上当受骗。当“把关人”门户大开，“恶之花”已出现在市场，消费者脑中的清醒和心中的理智就是保护自己的最后一道防线。

7月初，工信部的移动应用云测平台联合手机应用市场，为App提供质量评测。符合标准的App会在下载界面被标识为“高品质App”，这被视为官方出手监测App质量的一次良好尝试。若想促进手机应用产业的健康发展，需要建立统一的强制性监管标准，规范软件商店和应用开发者的行为。这样才有可能根除应用市场的乱象，明晰行业戒尺，走上健康发展之路。

(据《人民日报》)