设备加装预警模块、云控服务器远程监管……

提升物联网设备安全性需“内外兼修”

◎本报记者 张 晔

视觉中国供图

小到街头巷尾的监控摄像头，大到汽车、变电站，在万物互联和智能化的时代，物联网似乎能将一切实体都连入其中。根据中国产业信息网的数据及预测，2019年全球物联网设备数量已达107亿台，预计到2025年物联网设备连接数将达到251亿台。

然而随着物联网的普及，其安全问题也引发了人们的重视。近日，美国网络安全公司派拓网络发布报告称，该公司在日本智能太阳能发电板生产商日本康泰克公司的产品固件中发现了一个严重的安全漏洞，可被黑客用于网络攻击。此次发现的漏洞和其他20多个漏洞一起构成了派拓网络所描述的Mirai（米拉伊）僵尸网络的变体。

相较于传统网络，物联网在安全方面存在哪些不足？从此次安全漏洞事件来看，物联网想要持续发展，还要如何提升其安全能力？带着这些问题，记者采访了物联网安全技术领域专家和物联网领域相关企业负责人。

各种设备都会成为攻击对象

2015年，两名白帽黑客远程入侵了一辆正在路上行驶的某品牌汽车，他们利用该车型车联网接入系统的漏洞，对车辆的方向、油门、刹车、雨刷等进行了远程控制。当年7月，该汽车生产厂家就宣布召回140万辆存在漏洞的汽车。

类似的事件并非孤例。2016年，腾讯安全科恩实验室也曾利用安全漏洞对某知名品牌电动汽车进行无物理接触远程攻击，实现了对车辆驻车状态和行驶状态下的远程控制。这一结果也得到了该品牌汽车厂家的确认。

这两起车联网安全漏洞事件，背后指向的是整个物联网终端与日俱增的安全问题。

2020年，有研究者经过调查发现，仅半个月的时间，针对特定漏洞的物联网恶意代码攻击事件数量就达到了6700万次，有单个组织对数十万个IP地址发起攻击尝试，超过25%的安全入侵与物联网设备相关。从路由器到闭路电视摄影机，再到太阳能电池板，各种物联网设备都存在安全隐患。

南京邮电大学物联网安全专家沙乐天教授表示，目前物联网安全漏洞带来隐患主要有用户敏感信息泄露和恶意代码植入。前者表现为个人账号密码、用户照片及视频、用户语音被窃等，后者则表现为在路由器、摄像头、智能音箱、智能电视、智能网联汽车中安装木马程序，控制用户设备。

物联网安全建设面临挑战

近年来，电脑、手机等互联网终端的安全防护日趋完善，黑客对它们的攻击代价越来越大。而由于实体化的物联网设备发展时间较短，黑客攻击代价更小，因此针对它们的攻击逐渐增多。

沙乐天指出，物联网产业拥有产业链过长、设备多样性丰富等特征，如物联网产业链涉及物联网设备制造、传感器技术、通信网络、云平台、数据分析、应用开发和服务等各个环节，物联网环境下物联网设备品牌多样，通信协议也很多，这就导致体系化的物联网安全建设难以实现。“物联网设备还有一个特点是需要持续供电、长期运行，正常情况下不会频繁开关或重启，因此出现安全问题后难以实时进行检测。”沙乐天说。

物联网不同设备和系统的安全性也存在较大差异。南京中科智达物联网系统有限公司董事长许欣长期从事物联网通信设备研发，他表示，从连接方式来看，物联网设备分为蜂窝连接和非蜂窝连接两类，前者使用移动通信网络连入互联网，成本高、安全性也高，目前全球每年约新增4亿台终端，主要集中在智能网联汽车、电力等领域；而后者通过WiFi、蓝牙、Zigbee等连入互联网，使用开放频谱资源，成本低、安全性也差，全球约有110亿台终端，大多为智能家居设备。

同时，在物联网的云端、设备端和用户操作端之间，也缺乏统一的接入标准，这也带来了黑客攻击、数据泄露和隐私侵犯等潜在安全风险。

沙乐天表示，目前安全问题对于物联网产业发展的影响非常大。隐私数据的泄露或窃取降低了用户对物联网设备的信任，影响物联网设备的家用化普及。同时，针对物联网设备的僵尸网络远程攻击愈演愈烈，导致关键基础设施中的物联网设备使用率下降，极大影响物联网设备的工业化应用。

需完善整体协同防御体系

其实，物联网设备的安全防护并非不堪一击，但是新型攻击手段也层出不穷。与此同时，许欣表示，物联网发展正处于万马奔腾的阶段，各厂家提供的安全防护套餐也是丰俭由人，大多数只是针对通信端口的安全防护，属于基础防护，物联网整体的协同防御体系并不完善。

目前，针对物联网产品采取的安全保障主要通过“设备端+手机端+云端”的托管模式部署，这样既可以保证用户对设备的远程控制，比如在手机端查看家中的摄像头视频图像；又可以将设备访问权限的安全问题统一交托给远程的云控服务器，比如阿里云、华为云等平台。但从最新的安全漏洞及攻击事件来看，依然存在仿冒云端或手机端与物联网设备通信，从而实现对物联网设备非法远程控制的安全风险。

沙乐天认为，物联网要想持续健康发展，就应大力提升网络安全能力，从根本上解决设备端的安全风险。如在设备生产过程中加入入侵检测或漏洞预警功能模块，实时检测设备安全风险，并在发生安全风险时与远程的云端及用户手机端进行联动处置。同时，把物联网设备的安全管理模式同化到个人电脑终端，尽可能地解决网络安全的预警、检测及处置问题。

许欣告诉记者，可采取“主动出击”的方式提升物联网设备安全性。安全防控不应该是被动的，相关企业、高校和科研院所应展开合作，通过网络靶场的方式寻找漏洞，研发更安全的产品。

相关链接

独特安全机制护航物联网设备

与传统个人电脑终端相比，物联网设备具有许多特性，其面对的安全威胁和自身的安全性设计都与个人电脑终端有很大不同。针对于此，相关科研人员设计出了一些独特的安全机制。

例如，轻量级加密算法。由于物联网设备通常都暴露在不安全的物理环境中，且高度依赖于无线方式进行通信，因此加密算法对于物联网设备来说是一项“刚需”。然而，个人电脑终端等计算设备上常见的密码学算法在确保高安全性的同时，常常需要消耗数量可观的算力和能源。轻量级加密算法一方面可确保物联网设备的安全性，另一方面可降低其对算力的要求。

又如，设备指纹。设备指纹是设备的硬件和软件属性组成的一串信息。物联网设备的物理元件并非百分百相同，这导致物联网设备之间也存在着细微的物理差异，而这种差异恰恰可以作为一种特殊的“指纹”来使用。设备指纹具有唯一性，能够用于识别和跟踪设备的行为和活动，是安全风控的底层核心技术保障。

传统计算架构正失去竞争力

普慧算力开启新计算时代

◎本报记者 刘 艳

随着ChatGPT火爆全球，算力作为其幕后的核心引擎也走到了聚光灯下。近日，毕马威中国与联想集团联合发布《普慧算力开启新计算时代》报告。毕马威中国首席经济学家康勇在解读报告时表示，全球算力供给告急，传统计算架构正失去竞争力，人们必须探索新的计算模式。

当前，算力发展模式正发生转变，新硬件、新架构竞相涌现，现有芯片、操作系统、应用软件等都可能被推翻。

毕马威中国数字化赋能主管合伙人张庆杰表示，针对现实挑战，未来算力发展趋势将具备“数字经济的基础设施”和“通用人工智能的核心动力”两大特征，算力将在“普适”和“智慧”两个关键维度上加速发展，形成普慧算力。“普适”意味着算力将变得人人可得、人人可用、人人适用；“智慧”意味着算力将具备自适应、自学习、自进化的能力。

算力设施、算力应用、算力服务是普慧算力的三大关键要素。其中，算力服务代表着算力的提供方式，算力应用实现了算力的软件定义，算力设施是算力的基础。

报告以上述三要素为一级指标，进一步细分出13项二级指标，并首次搭建了普慧算力行业评估框架，将各行业的算力需求潜力分为四类，即以ICT（信息与通信技术）和制造业为代表的“普慧双驱型”，以汽车行业为代表的“智慧拉动型”，以金融业为代表的“普适促进型”，以及以医疗和教育产业为代表的“发展酝酿型”。

其中，制造业将成为普慧算力最大的潜在市场；汽车有望成为下一代移动智能计算终端，软件定义汽车的发展趋势要求算力实现智能化升级；金融行业将回归服务实体经济本质，“场景+金融”的模式要求接入广泛且灵活的安全算力；医疗和教育行业的算力需求当前还在酝酿阶段，但有望在普慧算力降本后迎来爆发。

位于天津市河北区的天津市人工智能计算中心为人工智能应用企业、高校和科研机构等提供普惠公共算力服务。图为在天津市人工智能计算中心中控室，技术人员在监控设备运行情况。

新华社记者 孙凡越摄

就医完成后款项即刻到账

区块链服务商保患者理赔

◎洪恒飞 李文芳 本报记者 江 耘

“叮咚”——随着手机短信提示音响起，杭州市民朱女士惊喜地发现，在她刚办理好浙江大学医学院附属邵逸夫医院（以下简称浙大邵逸夫医院）出院手续、还未走出医院门时，一笔1.3万余元的保险赔付款就已经打到了她的银行卡中。朱女士成为了区块链商保“零感知理赔”服务首批受惠患者。

7月15日，浙大邵逸夫医院在全国率先开展基于区块链的商保“零感知理赔”服务。患者无须进行手动理赔报案、提交材料，在就医时系统即可自动报案，进而实现从申请到结算理赔全程在线完成，就医完成后理赔即刻到账。

“区块链的核心，在于用技术架起多方信任的桥梁，从而促进正向循环和多方共赢。”浙大邵逸夫医院院长蔡秀军介绍，商保“零感知理赔”服务将帮助医院、医保和保险公司构建全新的数据共享信任机制，优化服务流程，提高保障效率，也将在“医疗—医药—医保”三医联动中发挥重要作用，助力完善多层次社会医疗保障体系。

记者了解到，该项服务依托浙大邵逸夫医院的电子病历医疗链应用与行业性区块链底层技术平台——“保交链”实现。医院与保险公司以“节点”形式接入区块链中，在获得合法授权的前提下，对患者身份信息、医疗记录、交易信息进行实时加密互信验证，实现相关数据信息的安全存储和传输。

在流程安全上，该项服务收集、使用数据遵循“一案一授权”原则，在获得患者合法授权后，仅允许保险机构收集和使用患者本次所需的医疗健康数据，其他数据“非必要不收集”，确保流程安全。

在数据安全上，该项服务依托的“保交链”为上海保险交易所自主研发的国产联盟链平台，它同时是国家级的区块链底层技术平台，具备全局化的国密算法、插件化的共识机制、产品化的智能合约、精细化的权限控制等功能，有力支撑了多边交易领域数据安全。

在网络安全上，该项服务基于“上海—宁波—杭州”跨省跨市专链，通过卫生专网接入医院内线，在网络边界部署访问控制设备，对访问节点进行控制。该项服务不仅对内网与外网进行了物理隔离以确保跨网数据传输安全，还可对网络节点进行实时监控，并能够建立网络应急预案保障网络安全。

蔡秀军表示，下一步，医院将继续深挖区块链与医疗行业的融合应用，在“零感知理赔”的基础上研发“零感知直赔”，在获得患者的合法有效授权后由保险公司直接赔付，解决就医“垫资”的问题，进一步减轻患者经济负担。

同等距离PB级数据传输时间由两周缩短至当天

CFFF平台为科研提供超强算力

◎本报记者 崔 爽

7月23日记者获悉，国内高校最大的云上科研智算平台CFFF（Computing for the Future at Fudan）近日在上海复旦大学正式上线。这台为发现和解决复杂科学问题而建的科研“超级计算机”由复旦大学与阿里云、中国电信共同打造，以先进的公共云模式提供超千卡并行智能计算，并支持千亿参数的大模型训练。

中国科学院院士、复旦大学校长金力表示，在数据和智能技术驱动的“大科学时代”，如何在日新月异的科技创新环境中赢得主动，在关键领域取得创新突破，是时代给予高校的命题。以CFFF平台为代表的智算平台作为一种新兴的科研超算架构，将成为科研的重要支撑力量，极大提升科研效率、降低科研成本，加速科学原理发现和技术突破，并有力推动科学大模型的落地。

云上传云上算 真正用好科研算力资源

据了解，CFFF平台由面向多学科融合创新的AI for Science智能计算集群“切问”一号和面向高精尖研究的专用高性能计算集群“近思”一号组成。

复旦大学“浩清”教授、人工智能创新与产业研究院院长漆远介绍，基于百G高速数据传输网和阿里云的大规模异构算力融合调度技术、分级存储技术、AI与大数据一体化技术，部署在复旦校内的“近思”一号和托管在1500公里外阿里云乌兰察布数据中心的“切问”一号连成了一台真正意义上的“超级计算机”。该平台可被复旦各校区所有实验设备高速接入，实现了异构算力统一管理，计算任务统一调度，满足了不同应用场景下的科学智能研究与应用需求。

此外，该平台还拥有国内高校最大规模的多级数据冷热分层存储集群，并支持云上高速传输。以往PB级科研数据从复旦大学传到西部数据中心需要两周，如今当天就能完成，实现了“东数西算”。

金力表示，CFFF平台具有大规模、高能级的特点。它是国内高校中规模最大的超算集群，同时也是国内高校算力第一的异构智算集群，以其为基础的智能计算平台将成为科研的重要支撑力量。

产学研共创新 研究进入计算驱动时代

“算力是人工智能学科发展的最基本保障。CFFF平台运行的速度将极大地影响科研效率、科研成本、平台的服务效能，以及未来算法产业化落地的可能性。”金力表示，大量前沿科学攻关领域，包括蛋白质计算、分子动力学、计算物理学、大气海洋地球系统模拟、气候变化综合评估模型模拟等都严重依赖算力资源。

据悉，CFFF平台从建设的第一天起，就收到了生命科学、大气科学、材料科学等领域的多种研究需求。

“CFFF平台的上线让我们像拥有了一个‘大科学装置’。实验科学的数据非常多，如果可以通过文献数据找到设计一种材料的最佳路线，不仅将省掉很多时间，也会使我们对物质的认识更加深入。”中国科学院院士、复旦大学化学与材料学院院长赵东元充满期待。在他看来，科研范式已经到了研究复杂体系的新阶段，必然要借助更多工具、不同学科的交叉融合来共同推进科研进展，人工智能就是一个很好的工具。

> 以CFFF平台为代表的智算平台作为一种新兴的科研超算架构，将成为科研的重要支撑力量，极大提升科研效率、降低科研成本，加速科学原理发现和技术突破，并有力推动科学大模型的落地。

目前，CFFF平台上的第一个科研成果已经诞生。复旦大学人工智能创新与产业研究院研究员李昊带领团队发布了45亿参数量的中短期天气预报大模型，预测效果在公开数据集上首次达到业界公认的欧洲中期天气预报中心（ECMWF）集合平均水平，并将预测速度从原来的小时级缩短到3秒内。李昊介绍，这样规模的大模型只用一天就完成了训练，传统的计算平台很难做到。

这是CFFF平台上孕育出的第一个大模型。金力表示，希望基于CFFF平台建成一批具有世界影响力的科学大模型，例如生命科学大模型、材料科学大模型、大气科学大模型等。未来，平台还将持续扩大其算力规模，并向复旦大学以外的科研机构、高校、医院、高科技企业等开放。

“高校第一次拥有了和科技巨头一样的研究计算平台，研究真正进入了计算驱动的时代。”中国工程院院士、阿里云创始人王坚表示，这也是产学研协同创新的成果，纵观技术的发展，特别在计算以及通信领域，“高校和企业可以创造出很多很美妙的东西”。