“间谍芯片”疑云:谁在撒谎?警示何在?

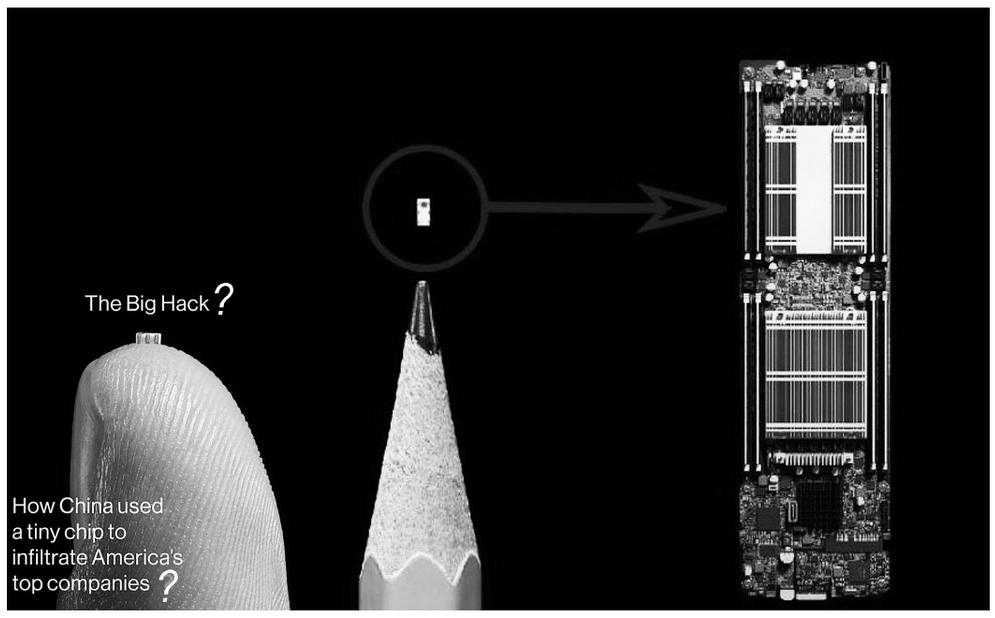
■本报记者 赵广立

10月5日起,一则“苹果、亚马逊被卷入,中国黑客利用微芯片入侵美国”的消息不胫而走,消息所波及的中美科技企业的股价应声下跌。而该消息的源头,来自于美国“权威媒体”彭博新闻社一则题为《大黑客:中国如何用迷你芯片入侵美国公司》(The Big Hack: How China Used a Tiny Chip to Infiltrate U.S. Companies)的封面新闻。

在彭博新闻社的这篇报道中,这枚“迷你间谍芯片”不足米粒大小,仅仅“与削尖的笔尖”相当,但微小身躯丝毫不影响它所蕴含的巨大能量。该封面文章称,该“间谍芯片”结合了足够的内存、网络连接能力和处理能力对宿主服务器进行黑客攻击。此外,在用伪装躲过检测的同时,在“服务器被打开时,微芯片改变了操作系统的核心,使其能够接受修改”。

也就是说,如果彭博新闻社的报道属实,这可能是有史以来公开报道的一个国家最大的硬件漏洞。

不过,无论当事科技巨头及外界各方的反应,还是从技术细节上的推演分析,彭博新闻社这则“经过2000名记者和多层编辑花了十几个月来组稿”(美国专业IT杂志 *The Register* 推特发文)的惊天报道,都越来越像一出自导自演的闹剧。



芯片级安全没有终点。 图片来源:360图片网

各方回应:子虚乌有

根据彭博新闻社“援引参与此事件的美国政府和私营公司的近20个匿名消息来源”的描述,这起“间谍芯片”事件始于3年前,中国某代工企业通过在Supermicro(超微公司,美国最大服务器生产商之一)的服务器某主板中植入一枚超级微小的芯片,进而黑进了全美约30多家企业的服务器里窃取信息,包括苹果、亚马逊。其中,亚马逊公司更是在该报道中作为“率先通过自查发现隐患”的案例被详细呈现。

作为这次所谓“间谍芯片”事件中首当其冲的公司,超微、苹果、亚马逊在该报道发出后迅速反应,发表清晰无误的声明否认有此事件,称彭博新闻社的报道是子虚乌有、无稽之谈。

超微公司在官方声明中回应称:“虽然我们会配合任何政府调查,但我们对任何有关这类问题的调查并不知情,也没有任何政府机构在此方面与我们联系过。我们也并不知晓有任何客户放弃美超微作为供应商是因为出现了此类问题。”

苹果公司则声称,“我们可以非常清楚地表示,苹果从未发现任何服务器中被故意植入恶意芯片、硬件操纵或漏洞”,还提到苹果“在过去的一年中,彭博新闻社曾多次与我们联系,声称发现了涉及到苹果的安全事件”,但苹果公司根据他们的询问进行的严格内部调查显示,“每次我们都没有找到任何证据来支持他们”,“几乎驳斥了彭博社此次有关苹果报道的方方面面”。

此外,美国公司高级安全官员还于当地时间10月7日致信美国国会,称他们没有发现任何证据表明中国黑客通过芯片对该公司进行攻击。苹果公司信息安全副总裁史塔克普洛斯向媒体透露,“苹果的专有安全工具会不断扫描这种出站流量,因为它表明存在恶意软件或其他恶意活动,但从来没有发现过类似情况”。

亚马逊也就彭博社报道中提及的“细节”严词回应,称“供应链妥协、恶意芯片问题或硬件修改的说法并非事实”,“关于亚马逊早就发现含有恶意芯片的服务器或基于中国数据中心的修改行为,以及亚马逊与FBI合作调查有关恶意硬件的数据,也从未发生”。

出人意料的是,10月6日,美国国土安全部在其官网上首度发声声援上述企业,表示“没有理由怀疑苹果、亚马逊和Supermicro否认此前彭博发布报道中的指控”。而据英国《每日电讯报》网站报道,英国国家网络安全中心也“支持美国科技企业苹果和亚马逊对彭博新闻社报道的否认”。

技术分析:可能性极小

根据彭博新闻社该报道发布的内容描述和图片信息,有硬件设计领域技术人员试图通过技术推演尝试验证该“黑客攻击”的可能性。在知名无晶圆厂半导体公司Marvell做芯片研发的硬件工程师“千载周瑜”(应采访对象要求化名)在推演后告诉《中国科学报》记者:“以目前的信息来看,(彭博社的报道)假新闻概率很大。”

他给出了3条技术理由。首先,数据中心在给服务器联网之前,通常会将智能平台管理接口(IPMI)中的基板管理控制器(BMC,彭博社报道中植入芯片的“可能所在”)的固件连同系统基本输入输出系统(BIOS)一起更新到最新版本;其次,在一个具备内网隔离和虚拟专用网络(VPN)的正常设置里,BMC连接根本无法访问互联网,外界也同样感知不到这个BMC的存在——这是一个“薛定谔的恶意后门”;第三,假设后门运行良好,那它一定会接受外界监听者的指令,并把监听的数据传给监听者进行数据分析——因为母板存储空间有限。但是这种大量数据的流入/流出,会被防火墙视为不正常,“但苹果或亚马逊这样的公司居然没人注意到(不正常的流量异常)?可能吗?”

为了进一步推演,“千载周瑜”做了一些假设,以让“间谍芯片”看起来可行。

通常,当个人计算机出现故障时,我们会重启或重装系统;而当数据中心的机器出现故障时,管理员一般不会亲自走到机器前,而是借助智能平台管理接口中的BMC,通过远程网络来重启/重装程序。

“如果植入芯片被放在BMC和包含BMC固件的串行外围接口(SPI)闪存芯片之间,那么它可以利用SPI的简单低频打个时间差,对SPI通信进行拦截或修改,甚至改变启动路径(Boot Path)。不过,具体植入芯片能发挥多大的作用,要看超微公司母板的硬件设计具体把多少功能交给了固件。”千载周瑜说,这里需要假设在母板中固件拥有过多的覆盖权限(假设一)。

其次,为了让植入芯片的每个引脚既能侦听又能篡改通信信息,还要假设植入芯片在引脚上有很大的电流来驱动(假设二)。而为了接触敏感数据或植入更强的木马,植入芯片还要通过干扰BMC与SPI闪存之间的通信,来篡改SPI闪存固件(假设三)。

“实际的恶意固件代码会在BMC上跑。BMC本身就是一个处理器,而SPI flash里的固件就好比它的操作系统。理论上BMC能读写服务器硬盘,只要BMC受到控制(假设四),就可以接触敏感数据或植入更强的木马。”

千载周瑜做了这一番假设后表示:“通过这番表述,想必读者也能大致了解到,让植入芯片成功运作需要多少假设和机缘巧合。”

记者了解到,彭博新闻社的报道里描述了超微公司雇佣了很多中国大陆和台湾地区的工程师,他们“用普通话开会,开会所用的幻灯片里包含中文,甚至还会在公司订中式糕点”,以此影射该公司在其所勾画的“间谍芯片”事件中存在猫腻。对此,千载周瑜表示:“一家由一群中国人创业的公司,开会还不能讲普通话?Slide(幻灯片)里还不能有中文?还不能订中餐?可见彭博社的这篇报道除了子虚乌有,已经没什么可写的内容,而这段描述在我眼里就是赤裸裸的种族歧视。”他还重申:“彭博社如果给不出后续证据,这篇报道一定是假新闻。”

10月9日,彭博新闻社发布了第二篇有所谓“新证据”的报道。文中提及“检测到被篡改的Supermicro服务器实际上作为两个设备出现在网络中”,“间谍芯片”通过“合法服务器以一种方式进行通信,另一个则以另一种方式、但所有流量似乎都来自同一个可信服务器”来使它得以通过安全过滤器。

对此,千载周瑜告诉《中国科学报》记者,他也注意到这篇新的报道,但他认为该文充斥着“大量文科生语言”,上文提及的“唯一有点技术含量的内容,没有成立的可能性”。

芯片级安全须重视

而对于《中国科学报》提出的“能否从技术上分析该‘间谍芯片’的可行性”问题时,天津飞腾信息技术有限公司一位要求匿名的高级工程师表示:“没啥想说的,感觉就是个假新闻。”

众所周知,中国的IT基础设施中布满了美国的各类芯片、IC器件,芯片设计和研发能力远在美国这样的超级强国之后。如果要通过硬件黑入IT系统,谁攻谁防的态势一目了然。对此,该高级工程师表示赞同:“如果这条新闻是真的,美国不是更有能力和条件来入侵中国IT设施吗?”

“大家稍微动动脑子就可以得出这个推论。他们无非是想给本国禁售中国IT企业产品找点安全借口。”该高级工程师告诉记者。

事实上,“硬件木马”并非不存在。早在2016年,来自密歇根大学的研究人员证明了在芯片制造过程中植入硬件木马的可行性,并在当年的电气和电子工程师协会隐私与安全大会上进行了演示,而当年他们的研究还在该会议上获得了最佳论文奖。

在那篇获奖论文中,密歇根大学的研究人员称,他们的本意是防止这类无法检测的硬件后门攻击,而不是发明它们。“事实上,世界各国的政府有可能已经想到了这种模拟电路攻击方法。”他们写道,“通过发布此论文,我们声明,这种攻击是真实的、迫在眉睫的威胁。现在我们需要找到一种防御方式。”

“尽管有很多技术细节需要弄清楚,但它展示了芯片级安全的重要性:不仅要防,也可以攻。”中科院计算所研究员韩银和表示,这一事件提示我们,芯片级安全须加以重视。

那么,在芯片产业中尚处于弱势的中国如何保障硬件安全?“第一,尽量采用国产关键软硬件;第二,要重视和加强IT产品的安全检测。”上述高级工程师表示,尽管目前针对硬件木马的检测技术是在不断演进的,但道高一尺魔高一丈,安全没有终点。

声音

『新杭州故事』只是个开始

■赵广立

在今年的2018杭州·云栖大会上,杭州市政府联合阿里云等企业建设的杭州城市大脑2.0正式发布。经过1年的投用,城市大脑已成为杭州新基础设施。根据阿里云提供的数据,目前的杭州城市大脑管辖范围已扩大28倍,覆盖全城420平方公里,相当于65个西湖大小;而通过交警手持的移动终端,城市大脑可实时指挥200多名交警;在城市大脑的作用下,杭州交通拥堵率从2016年的全国第5降至2018年的全国第57名。

除了依靠大数据、人工智能摆脱拥堵,今天的杭州还是“移动支付之城”“移动办事之城”“智慧医疗之城”。

在杭州,出门办事“最多跑一次”。全市59个政府部门368.32亿条信息汇聚在基于阿里云打造的政务服务平台上,市民可凭身份证一证通办296项事务。

在杭州,超过95%的超市便利店、超过98%的出租车、5000余辆公交车都支持移动支付,堪称全球最大的移动支付之城。

在杭州,去医院做CT,不再需要去固定医院就诊,也不需要将片子全部打印出来;智慧医疗让近7000万人次在杭州市属医院看病时间平均缩短2小时以上。

在杭州,法院审理某些案子不再需要原告被告到场,甚至不需要书记员;航运、港运、路运师傅不再需要花很多时间办各种各样的证件;而创业公司也不再需要自己搭建服务器、数据中心,每天只需几十块钱就可以享受与大公司一样的计算服务。

而这些“新杭州故事”,明天将会在更多城市发生。在阿里云总裁胡晓明看来,杭州正在被打造为数字中国的标杆城市,但“新杭州故事”的意义不止于杭州。

城市的优化背后是科技的助力,而如今实实在在发生在杭州的故事,明白无误地显示,由于数字化技术的全面渗透,杭州这座人文之城已经变成了科技之城。而人文与科技的融合,正是人们对城市繁荣的一大向往。

不过,参与到这一科技进步创新进程的,不仅仅是科技公司数以万计的工程师,还有政府的推动,以及这些技术的受众、千千万万的普通人。“新杭州故事”证明了一件事,要拥抱数字化生活,需要从政府、企业到市民的参与,全面拥抱数字经济,才有美好故事的发生。而要让“新杭州故事”不仅仅发生在杭州,还需要推动科技产业化,把越来越多的技术能力带到华夏大地的各个角落。

按图索技

HyperloopTT推出世界首款全尺寸超级高铁乘客舱

10月2日,在西班牙圣玛利亚港举行的揭幕仪式上,超级高铁公司Hyperloop Transportation Technologies(下简称HyperloopTT)揭开了其全尺寸超级高铁乘客舱的神秘面纱。

被命名为“Quintero One”的乘客舱,几乎全部由HyperloopTT自主研发的智能泛合金材料打造,并在HyperloopTT的合作伙伴Airtificial公司位于西班牙南部的航空航天工厂制造。该乘客舱的设计工作则由HyperloopTT与世界著名运输设计咨询公司PriestmanGoode通力协作完成,并一举荣获“2017年英国伦敦设计奖”金奖。

“Quintero One”乘客舱长32米、内舱长15米,舱重5吨,内置有72个传感器和75000个铆钉。该乘客舱将被送到位于法国图卢斯的HyperloopTT超级高铁研发中心进行额外组装并整合到系统中,为HyperloopTT超级高铁的首次商业轨道使用做准备。

据HyperloopTT授权国内机构发布的信息显示,HyperloopTT5年来已经“解决并改进了”包括“全新的悬浮系统、真空泵、电池和智能复合材料等”在内的“超级高铁所需的所有技术”,加之相应的安全认证指南和保险框架,HyperloopTT“现在已有充分资格将超级高铁引入世界”。

此外,HyperloopTT联合创始人兼董事长Bibop Gresta表示,乘客舱还将于2019年“全面优化”,为乘客安全高速出行整装待发。

(赵广立)

专家视点

拥抱工业互联网的正确姿势:

业务驱动,“造一把可靠的锤子”

■王晨

当前,大数据已成为业界公认的工业升级的关键技术要素。马云在云栖大会上也表达了以前制造业靠电,未来靠数据的观点。在“中国制造2025”的技术路线图中,工业大数据是作为重要突破点来规划的,而在未来的十年,以数据为核心构建的智能化体系会成为支撑智能制造和工业互联网的核心动力。

工业大数据的重要性众所周知,但究其根本,大数据是手段而不是目的,人工智能也是如此。如果仅仅因为工业互联网的概念很热,企业就要去盲目拥抱工业互联网和工业大数据、人工智能技术,实际上是一个非常错误的观点。

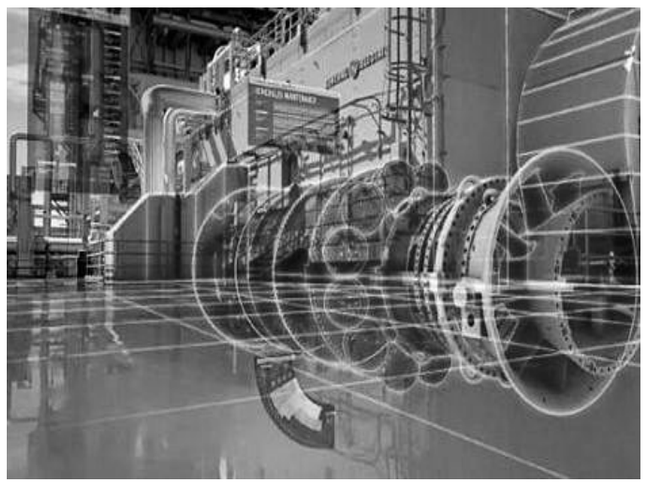
工业从数据到大数据

在新一代信息技术出现之前,工业企业已经正常运转了上百年,我们应该清晰地认识到信息技术手段的加入更像催化剂的作用。首先需要明确需要达到怎样的业务目标,可以使得今天已经存在的生产工艺、工业产品、管理方法变得更好。

其实大数据支撑制造业的业务变革最根本的目标就是提质增效,在自动化与信息化基础之上,实现智能化的制造体系。在智能制造的基础上,然后才是打造平台,构建产业生态,与产业链进行更有效的协同,实现工业互联网的乘法式发展。

工业大数据的三个典型应用方向,也是我们实现工业互联网的目标,包括智能装备、服务型制造和跨界融合。第一个层次是设备级的,就是提高单台设备的可靠性、识别设备故障、优化设备运行等;第二个层次更多是针对产线、车间、工厂,提高运作效率,包括能耗优化、供应链管理、质量管理等;第三个层次是跨出了工厂边界的产业跨界,实现产业互联。

工业大数据并不是凭空而来,传统工业信息化一直在进行,我们已经有大量的数据来自于研发端、生产制造过程、服务环节,工业信息化过程一直在产生大量的数据,工业从数据到大数据,其实更多要考虑的是与自动化域数据的叠加,这是数据的两化融合。而在工业互联网时代,我们还需要纳入更多来自产业链上下游以及跨界的数据。



工业大数据有哪些特点?我们总结为“多模态、高通量、强关联”的特性。我们在工业领域总结了约有130多种不同类型的数据,数据模态多样,结构关系复杂。高通量是指数据持续不断地产生,采集频率高,通量大。强关联是指工业场景下的数据有非常强的机理支撑,不同学科之间的数据是在机理层面的关联,而不是数据字段上的关联。

而对工业大数据的分析应用,也不是将深度学习、强化学习的方法放到这里就可以有结果。我们需要获知研究对象的机理模型与定量领域知识,而这在当前基础上前进很困难。我们希望找出数据在输入、输出之间的统计关系,对机理和模型不确定、不清晰的部分加以补足,这是工业大数据应用的基础。

业务引领,数据推动产业发展

智能制造在不断获得数据的驱动,从智能制造到工业互联网平台,核心都是利用数据和模型,优化制造资源的配置效率。

工业互联网并不等同于智能制造,区别在于数据的跨界和业务的边界上是否有所突破。当下,太多人过于重视平台能力,而真正的工业互联网讲的是生态,资源优化从描述、诊断向预测、决策不断深入,从单机设备、生产线、产业链再到产业生态不断拓宽。

我们的生态如何来构建业务体系,如何跨界,才是工业互联网成功与否的关键。而决定工业互联网发展方向的,一定是业务驱动。我们从一开始就反对拎着一把锤子,满世界找钉子,现在很多大数据、人工智能公司就存在这个问题。

我们需要深入到一个工业领域,造一把可靠的锤子,刚好可以去敲有需求的钉子,业务驱动和问题驱动才是产业发展的本质,而不是技术驱动。将业务、数据理清楚,评估数据,真正实现业务落地,要点就是三个要素的协同——人、场景、算法。

(作者系清华大学大数据系统软件国家工程实验室总工程师,本报记者贡晓丽据其在中国计算机学会青年计算机科技论坛工业互联网与边缘计算专题探索班发言整理)