“间谍芯片”报道提示安全观须更新:

中国如何应对硬件供应链安全挑战

■本报记者 赵广立

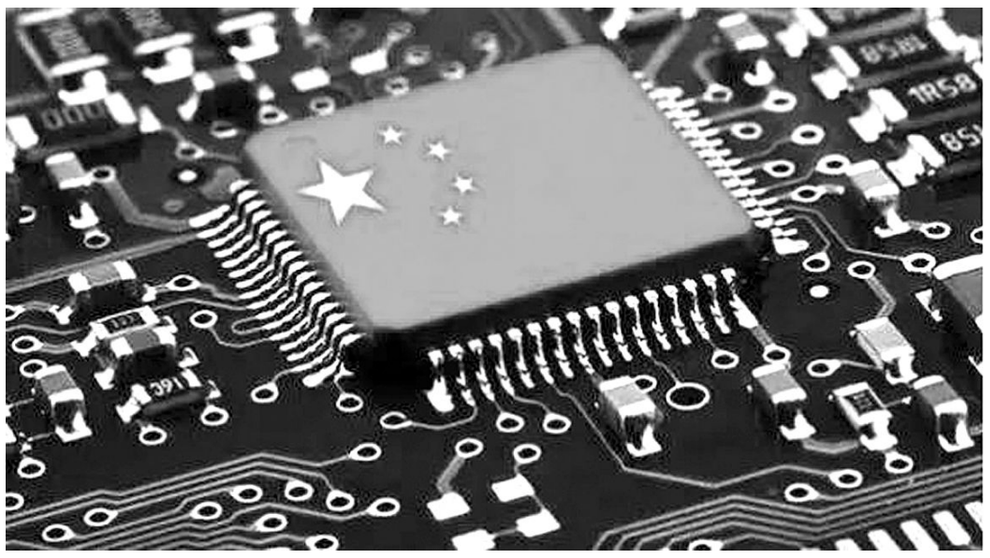
继彭博新闻社10月9日更新了其所谓的“中国黑客利用间谍芯片攻击美科技公司”的报道之后,业内专家分析认为该事件的真实性越来越离谱。然而,诡谲的是,该事件给各方带来的负面影响却越来越大。

“10月4日彭博新闻社报道刚出来的时候,指责所谓‘中国黑客’利用伪装芯片发动攻击的方式,经济上不合理、技术上又太复杂,我是不怎么相信的;10月9日彭博社进一步指摘‘黑客’在网卡接口处隐藏‘间谍芯片’,却又没有证据来证实这一点。”360集团技术总裁兼首席安全官谭晓生在接受《中国科学报》专访时说,彭博社前后两次报道提及的“黑客攻击”非常难以证伪——不可能把彭博社所指摘的所有主板都拆来检视,但也无法证实——彭博社并没有拿出实证,且其所取信的信源也没有可信度。

“总体感觉是被泼了脏水,但又很难自证清白,这就很痛苦了。”谭晓生认为,这种模棱两可的态度反而造成了坏的影响。

就在全球的技术专家都在忙着搞清这篇报道真相的同时,美国新闻界和民众却开始宣扬保护本国的“供应链安全”。如美国《大西洋月刊》和《国会山报》的文章都认为,“即便中国没有通过硬件入侵美国企业的服务器主板,彭博社的报道也暴露出了过于依赖中国的电子产品供应链条给美国带来巨大的安全危机”。

然而事实是,没有哪个产业比集成电路有着更鲜明的全球化烙印。如果说仅仅依赖中国的供应链就要承受“巨大安全危机”,那么无法想象每年进口全球芯片50%以上的中国要承受什么。



没有哪个产业比集成电路有着更鲜明的全球化烙印。 图片来源:百度图片

硬件安全,易被忽视的问题

“(硬件安全)暴露出来的案例还不多,尚未引起足够的重视。彭博的这个报道实际上也给我们提了个醒。”中科院计算所研究员、计算机体系结构和芯片研究方向博士生导师韩银和在接受《中国科学报》记者采访时说,其实相比于软件安全、网络安全、数据安全等,硬件安全特别是从关键元器件发动的攻击,相当于一种新的“降维攻击”,要高度重视硬件安全的重要性。

谭晓生也告诉记者,芯片的确是攻破安全屏障的一个进攻点,而且因为它在最底层,如果有预置后门或埋了木马,幕后操纵者可以“一层层地向上打”。如果对这种攻击方式不甚了解的话,被攻击方很难察觉。

而从硬件出发,黑客可能从芯片层、电路板层、固件层发动攻击。

谭晓生介绍说,芯片级的主动攻击,可以做到与正常芯片外观、管脚、封装等都一样,但芯片内部电路被篡改。这种通过篡改原始集成电路设计,植入完成特殊功能的逻辑,业内称为芯片木马或者硬件木马。在满足一定条件的时候(如反复执行某个指令引起状态反转),木马会被唤醒,进而实施改变功能、窃取信息、物理摧毁、协助软件木马控制系统等攻击行为。

韩银和对记者说,2016年美国密歇根大学研究人员在IEEE安全领域顶级会议之一IEEE隐私与安全大会上已经证实,在芯片制造过程中可以植入硬件木马。在这次大会上,研究人员公开了一种只需要几十个门电路(整个芯片大概为几十亿个门级)的超小型硬件木马,这种木马可通过运行一系列“看上去完全无害的命令”触发处理器某项功能进而获得操作系统完整权限,危害极大。

更值得担忧的是,韩银和指出,该芯片木马只要芯片制造工厂中的一位员工就能进完成植入,而且基本无法通过任何现代硬件安全分析手段检测出来。

类似的,与芯片共同构成电路逻辑的电路板乃至执行某个特定功能的固件(介于软硬件之间),都有可能被植入恶意逻辑,这些同样非常难以发现。

“限于工艺能力,中国许多芯片在境内设计、在海外流片,在流片的过程中,如果有别有用心者对芯片做了手脚,检测起来也是非常难的。”谭晓生告诉记者,从这个角度来讲,对于供应链安全,中国才是最该担心的。

韩银和更是直言,硬件木马对于我国威胁更大:一方面该木马可以在制造阶段插入,由于半导体高端制造环节都在国外,这一隐患更大;另一方面,现有高性能芯片是非常好的硬件木马宿主,而我国无论是高端信息服务业和重要行业,每年都从美国进口大量的高端处理器。

中国如何应对硬件安全?

中国是全球最大的芯片进口国,全世界50%以上的芯片进口到中国。

海关总署公开信息显示,2017年中国集成电路进口量高达3770亿片,同比增长10.1%;进口额为2601亿美元(约合17561亿元),同比增长14.6%。集成电路进口额占中国总进口额的14.1%。

随着智能物联网设备的爆发式增长,中国未来只会进口更多的芯片。而随着更多的设计者、生产者进入芯片产业链条,几家大公司垄断的格局也将被打破。当“企业信誉”变得更为复杂,则意味着供应链全流程中安全漏洞更多,甚至可能产生与软件领域那庞大的黑灰产业。在此背景下,中国如何对硬件安全挑战?

“安全问题不可能完全杜绝,至少现在从理论上没有绝对安全的计算机系统,只是攻防难度不同。”中科院计算所研究员、先进计算机系统研究中心主任包云岗在接受《中国科学报》记者采访时提出,就像我们追求健康一样,要有适当的手段来防止“病入膏肓”:不是绝对不生病,而是病痛来临之时能防能治。

投射到硬件安全方面,就是要找到性价比最高的安全保障方案——花合理的钱保障足够的安全。怎么做到这一点?“个人观点,更重要的是构建免疫系统,就是有未知入侵,也能很快识别,并快速响应减少危害,形成免疫。”

问题是,怎么构建这个免疫系统。

“这就需要核心技术了。”包云岗说,可以参考人体的免疫系统来研究相应的一整套技术系统,比如类似B细胞的识别入侵机制、T细胞的有效杀死病毒;当B细胞和T细胞被激活后,会形成免疫记忆等。

在韩银和看来,上述提到的“免疫系统”应该既包括“防”又包括“攻”。

“相关技术体系的构建也不能仅仅关注防守,也要重视‘攻’的技术,‘攻’的技术进步可以大大提升防守的能力。”韩银和对记者说,美国在这方面非常重视,而且有可能有成体系发展“芯片武器”的计划。相比而言,我们的研究还不够系统。

同时,韩银和还提示,面对潜在的硬件安全挑战,我国还应该建立健全供应链安全管理体系。“企业作为主体,建立关键元器件和系统可信审计制度,建立对芯片制作全过程的跟踪体系,避免伪制和过程中的恶意电路添加。”

现有技术能防御几多

硬件安全威胁重大,目前对其也并非完全束手无策。谭晓生告诉记者,芯片安全保护除了硬件检测外,还可以利用已有的网络安全技术实施防御。

“不论是芯片级、主板级还是固件级的攻击,它就算隐藏起来,也始终是一个‘坏人’。坏人总得干‘坏事’,而只要它干‘坏事’,就一定会留下一些行为上的特征:如功耗变大、网络流量异常、行为异常等。”谭晓生对记者说,通过一项名为边信道检测的技术,就可以检测到电流、噪声、电磁等的变化。

此外,通过网络行为检测和应用程序检测等多维度信息的收集,就会有更高概率发现恶意程序造成的机器异常,进而分析机器运行的程序是正常程序还是木马。

“这其实就是攻防维度之争。攻击者能控制多少维度、防御者能控制多少维度,二者对比可见高下。如果说作为防御者,有一些维度是攻击者无法控制的,那么就有可能通过这些维度检测到攻击者。”谭晓生说。

360网络攻防实验室负责人林伟介绍称,360今年发布的“安全大脑”就是这样一种理念:在无法判断哪些行为是攻击的情况下,尽量多地对行为和数据进行记录,然后对这些海量数据进行存储、分析、挖掘和关联,并配合人工智能技术,快速发现高级威胁。

“网络安全领域有个理念叫做‘零信任’,说白了就是‘啥都不能信’。在整个安全防御体系里,相信什么,可能就会‘死’在什么上面。”谭晓生对记者说,追求“零信任”,其实是追求全维度的分析检测,这需要大量的存储、计算和分析。所幸,随着近年来计算和存储成本的下降,“安全的钱舍得花了”。

不过,韩银和认为,要应对硬件安全挑战,我国在科研上还应围绕硬件安全组织开展方方面面的研究。

“国内已经有一些研究团队开始关注芯片安全的问题。中科院计算所在几年前成立集成电路安全团队,并已经取得了一些突破性的工作。但相对于国外研究,我们起步晚了一点。”韩银和说,由于硬件安全的危害性还没有完全展现出来,所以目前我国投入和重视程度都不足。

“这体现在研究上系统性不足,成果的核心技术主要集中在一些点的技术上,而且偏重于‘检’和‘防’的技术,而芯片木马‘攻’的技术也很重要,只有建立完整的“攻—检—防”技术体系,才能综合发挥作用。”韩银和说。

延伸阅读

美国对『供应链安全』早有防备

美国历来关注和重视供应链的硬件安全问题。

过去,美国军方在IBM有一条专门的生产线,用于向军方提供相应的芯片。后来,IBM把这条生产线卖到了中东,这使得美国军方非常抓狂,因为这意味着其芯片的生产商不再是美国公司了,其可靠性就成了一个大问题。自此之后,美国对有关芯片安全的检测技术等非常重视。

早在2012年,美国国会就有一个关于美国国防供应链中仿制芯片的报告,重点分析了美军供应链中的仿制电子元器件问题。该报告介绍了在2009年到2010年两年的时间,美军发现了1800多例伪造电子元器件事件,涉及100多万个分离元器件。后来,美国国防部高级研究计划局联合几家大学和研究机构,启动了一项名为“国防可信硬件电子供应链(SHIELD)”项目,该项目的主要目的就是消除在美国国防电子产品供应链中的伪造芯片。

伪造芯片也是芯片安全中的一大类。其危害轻则可能存在可靠性问题——由于采用了比较廉价而低质的芯片,造成整个电子系统的可靠性存在隐患。如果是在伪造芯片过程中插入一些恶意电路,则相当于植入了芯片木马,危害就更大了。

目前可以检测芯片木马的手段包括切开芯片用高微显微镜观察内部逻辑,用激光探测判断内部结构、电路运行情况等。但现在的芯片结构已经非常复杂,即使这些高科技的检测手段,也需要耗费极大的成本才能检测到木马。

值得一提的是,当下芯片木马先进的检测技术和设备都在美国,美国国防部下属的国防高级研究计划局在2007年和2010年连续启动了“可信性集成电路”和“集成电路的完整性和可靠性”两个项目,鼓励大批科研人员重新审视集成电路的安全性和完整性问题,并投入到硬件木马电路检测和研究领域。

相比之下,中国在芯片设计和生产领域和美国存在较大差距。

美国佛罗里达大学芯片安全专家金意儿教授曾表示,在处理器设计领域,中国与国际先进水平仍有一定差距。所以在处理器、SoC(片上系统)的设计过程中,不得不大量使用第三方提供的IP核,或者受工艺的限制将设计拿到海外进行流片。

然而,在整个处理器和SoC的设计生产过程中,芯片受到硬件木马攻击的机会很多。攻击者很轻易通过这些硬件木马电路获取武器系统、银行系统等内部机密信息。

(本报记者赵广立根据采访整理)

按图索技

①液态SICN前驱体
②3D液晶显示系统
③通用捆绑验证平台

新科技亮相第四届军民融合发展高技术装备成果展

10月8日至15日,第四届军民融合发展高技术装备成果展览在北京举办。本次展览共设置综合区、先进材料区、先进制造区、新能源区、自主可控区、信息发布区和中大型实装区七个展区,重点展示了我国近年来在“先进材料”和“新能源”领域具有自主知识产权的核心关键技术。北斗卫星系统、3D打印、航空发动机、前沿材料等一批新技术新产品亮相展会。本届展览延续了专业展的特点,分别安排了“先进材料”、“先进制造”和“新能源”三场专业论坛和签约活动。

军委装备发展部科研订购局副局长李欣欣表示,这次展览主要突出了先进材料、先进制造、新能源以及自主可控这种战略基础性领域方面的产品。民营企业占了50%以上,此外,还有中科院、教育部高校、大中型国有企业等参展方,集中展示了这几年来各个领域军地双方共同努力取得的最新成果。

自主创新一直都是军民融合深度发展的力量源泉,在展会现场自主创新产品比比皆是,有些制造工艺达到世界顶尖水平,有些则弥补了国际领域空白。此外,一批具有新材料、新能源技术的科技企业,也在本届展会中首次亮相,它们把在民用中试点并推广的成熟产品,结合军队作战需求进行创新改造后带到了展会现场。

党的十九大报告中将军民融合提升至国家发展战略,截至2017年,军委装备发展部等部门共同推动制定了推进装备领域军民融合深度发展举措,包括具体任务和具体工作。其中36项已完成或基本完成,9项已按计划有序推进。 (赵利利编辑)

宁波市以民营经济为主体,著名高等院校和科研机构相对较少,因而高端人才缺乏,引进高端智力推动宁波经济发展成为当务之急。

院士工作站宁波之路:

高端智力为发展插上腾飞之翼

■本报记者 陆琦

在宁波鄞州高教园区内,有一组宏伟的景观:数米高的花岗石平台上,近百位甬籍院士的青铜雕塑三五成群,或相互交谈、或独自沉思、或举目远眺。这里就是宁波院士雕塑园。

宁波是全国闻名的“院士之乡”。现有甬籍院士116位,目前健在的还有89位。也就是说,在不到20位两院院士中,就有一位宁波人。

自2008年建立浙江省首家院士工作站至今,宁波已建院士工作站112家,共柔性引进海内外院士109位,引进院士创新团队140个、高层次专家950余名,为宁波建设国际港口名城、打造东方文明之都提供了强有力的人才保障和智力支撑。

高端智力引领优势产业发展

发展是第一要务,人才是第一资源,创新是第一动力。宁波市以民营经济为主体,著名高等院校和科研机构相对较少,因而高端人才缺乏,引进高端智力推动宁波经济发展成为当务之急。

2008年9月,宁波市院士服务和咨询中心正式成立,宁波高新区研发园区、浙江万里学院、中国兵器科学研究院宁波分院、宁波浙东精密铸造有限公司、中科院宁波材料所等5家单位成为宁波市院士工作站试点单位。

随后,宁波市院士工作站在不同区域、行业、领域涌现。

“院士为我们打开了实现创新驱动的一扇窗,让我们可以借此机会,实现经济效益和研发水平的同频共振。”宁波东方电缆股份有限公司在柔性引进黄崇祺院士团队之后,成功掌握了水下生产系统脐带缆、动态电缆、拖曳缆等国际先进海洋缆产品最新技术,承担了新中国成立以来行业内唯一的国家科技支撑计划项目和国家“863”计划项目,并牵头起草了海底电缆国家标准。

从2011年起,宁波伏尔肯陶瓷科技有限公司先后建立省级院士工作站、企业研发中心、博士后工作站,同时还成立技术创新团队,通过引进和培育科技人才、项目带头人,撬动企业创新发展。

这样的例子还有很多。无一例外的是,和院士团队达成合作的企业,几乎都是宁波优势产业内的引领者。它们深深地体会到:院士专家工作站是企业转型升级的“发动机”,为企业创新插上腾飞之翼。

创新资源集聚提升发展质量

“没有院士工作站,就没有伏尔肯的今天,更没有伏尔肯的明天。”谈到院士工作站对企业的帮助,伏尔肯公司总经理邬国平感慨地说。

伏尔肯公司是一家生产陶瓷密封材料的高新技术公司,在院士工作站的帮助下,该公司研制的飞机陶瓷刹车技术获得了2016年国家技术发明奖二等奖。邬国平说:“在院士工作站成立之前,我们只能看到眼前,有了院士工作站,我们站得高了,开始从科技创新的大格局上看问题了。”

引进一位院士及他所带来的高端人才团队,意味着创新资源的集聚,将推动某个行业乃至某个地区自主创新的热潮。

宁波市科协积极引导建站单位,根据院士团队智力资源和自身发展需求,创新拓展引智工作内涵,从单一为企业解决技术难题向开展战略决策咨询、协助引进及培养高层次人才、共建研发平台、合作申报国家(省)级重大技术合作项目等方面延伸,使引智工作成效得以进一步放大。

据统计,在院士团队帮助下,宁波112家建站单位建立国家级研发平台2个、省级研发平台55个、市级以上重点学科15个、市级以上重点实验室10个,申请市级以上科技项目850多项,获得国家发明专利授权900余项,参与制定国际和国家标准100余项,获得市级以上奖励300余项。

恰如薛群基院士所说,宁波极具文化底蕴,其民营经济和创业元素也非常活跃,加之其科学技术的发展态势,宁波将发展出自己的创新模式。

用心营造良好人才生态环境

人才竞争归根究底是城市综合环境的竞争。宁波精心打好“理念引智”、“情感引智”、“文化引智”和“服务引智”的组合拳,用心营造宁波敬才重才的人才生态环境。

宁波市委市政府主要领导只要能排出时间,均会亲自会见来甬院士和其他顶级专家。在1月份宁波两会期间,市委书记郑栅洁和市长裘东耀等领导还专门邀请院士代表召开座谈会,听取薛群基、赵玉芬、古洛夫斯基·瓦连京、徐志磊、都有为等8位在甬工作或建站院士的意见建议。

作为“院士之乡”,宁波不仅高度重视甬籍院士的联络联谊和智力回归,而且还积极通过全职引进院士、建立院士工作站、建立院士创新创业中心等方式大力引进海内外院士高端智力,助力宁波市高质量发展。

宁波市科协主席陈文辉打了一个形象的比喻:“科协就像接线板,接着国内外专家这个‘电源’,为有科技需求的企业‘供电’。”

2013年,依托浙江万里学院成立了宁波市院士文化研究中心,集聚社会各界力量一起推进院士文化研究。目前,该中心已经开展院士文化理论研究、甬籍院士与宁波地方文化和甬籍院士资料目录汇编等7个项目,并启动了“甬籍院士口述史研究工程”。

今天甬籍院士光荣与梦想的历程薪火相传、生生不息,明日宁波必将续写更为辉煌的发展篇章。