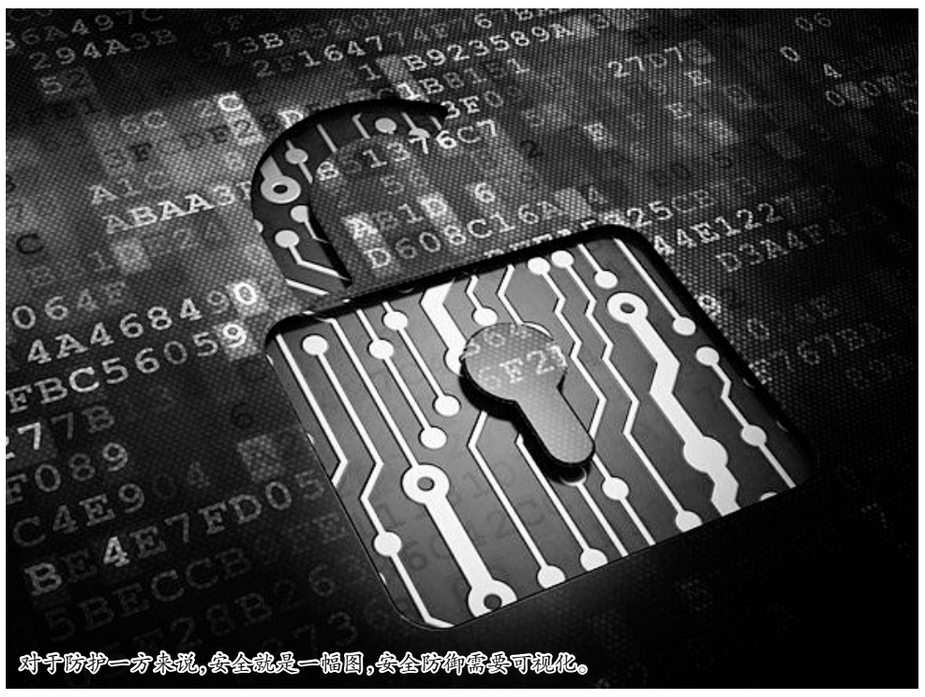
态势感知:变被动防护为主动出击

■本报记者 赵广立

二十国集团(G20)峰会召开在即,安全保障工作必须做在前面。

具体到网络安全方面,网络战场上“我在明敌在暗”,要确保网站特别是业务系统不被攻击,现实压力非常大。若此,计将安出?

亚信安全引入了“态势感知”理念和技术,变被动为主动防御黑客入侵。亚信安全TSG产品管理副总经理、移动安全专家刘政平告诉《中国科学报》记者,态势感知技术可以以图形或地图可视化的方式,把威胁的来源、攻击的手段、主要的风险以及可能影响的范围,甚至未来趋势勾划出来,做到对网络空间实时、动态地主动防护。



对于防护一方来说,安全就是一幅图,安全防御需要可视化。

被动防护落后一步

网络安全的防线有多脆弱?国际知名安全公司FireEye曾于2014年5月发布了一份名为《网络安全的最后防线:深度防御的实境评估》的研究报告。报告称,FireEye分析了全球1217家遭受安全攻击的企业。尽管这些企业广泛部署了诸如防火墙、IPS、沙箱或防病毒产品,但仍有高达97%参与调查的企业曾被黑客成功入侵。

问题出在哪里?

著名白帽子、阿里云云盾负责人吴翰清分析说,虽然这些企业部署了安全设施,但是安全设施感觉到黑客存在的时候往往是在入侵事件发生之后。当然,也有可以实时给予存在感的系统,但只是一大堆的告警。更专业一点地说,是混杂了大量误报和无用信息的信息轰炸——其实这和看不到没什么两样。

这是一件令人郁闷的事情:为什么总是跟在黑客屁股后面?

这种“看不到”并非偶然。在吴翰清看来,安全攻防完全可以用著名的“木桶理论”来解释。按照木桶理论,只有构成木桶的所有木板都足够高,木桶才安全;所有木板比最低木板高出的部分都是没有意义的,要想增加木桶的安全,应该设法增加最低木板的高度,这是最有效也是最直接的途径。因为,黑客总是会从意想不到的地方入侵。

因此,对于防护一方来说,安全就是一幅图,如果没有看整张图的视野,就等于什么也看不到。换句话说,安全防御需要可视化。

关于如何解决安全的可视化,国内外的安全专家已进行过大量的研究。一个关键的突破便是“态势感知”理念的引入。

动态的安全防护

公认的“态势感知”(SA,Situation Assessment的缩写)概念是,在特定时空下,对动态环境中各元素或对象的觉察、理解以及对未来状态的预测。其中,“觉察”又称为一级SA,本质上是“数据收集”;“理解”为二级SA,本质上是掌握数据中的情报;“预测”称为三级SA,本质上是情报的应用。

“态势感知”概念起源于20世纪80年代的美国空军,指的是军方通过对空战环境信息的分析,快速判断当前及未来形势并作出正确反应,无疑这对取得胜利具有决定性的作用。然而,信息安全领域要做到态势感知并非易事。

想要实现全面、快速、准确感知过去、现在、未来的安全威胁,首先要充分尊重原始数据,或者称之为基础数据。正是缘于无法获得所有这些基础数据,很多中小企业在“态势感知”面前望而却步。

“现阶段很少有中小企业涉及态势感知,真正有实力关注态势感知的是类似致力于‘平安城市’的成都市政府这样的城市运营方和金融、电力等基础行业的大型企业。”刘政平告诉记者,亚信安全目前也只是与这些“大客户”进行合作,原因就在于他们“有海量的真正的大数据”。

然而,有了这些数据,还并不等于可以精确地得知网络威胁。

“大数据有一个特点,就是价值的低密度。比如,现在在很多楼道里面都有摄像头,但是真正有价值的数据只有几秒钟的时间。同样的道理,黑客对业务系统的访问等数据或者一些攻击行为等也是隐藏在大量的日志文件里面,也是低频的数据,不是密集的攻击。”刘政平指出,这时候就需要平台方对软件运行日志等有非常深刻的理解和研究。

“代码比对技术、智能化报警等经验的沉淀积累也是很重要的。并不是说有了数据就可以很精确地告知入侵风险。”刘政平说。

此外,现在黑客都是动态的,每次攻击都不一样,用的手法、程序包也都是不一样的,因此需要通过感知系统推动设备自动产生一些安全策略阻断它们。

总体来讲,态势感知技术是一种动态的安全保护。“比如站在城市安全的角度,我们要保护的是基础设施,不能等到已经发生了严重的事情再来‘救火’。必须在黑客发动第一步攻击的时候就要联动到整个体系上的安全策略。”刘政平总结说,态势感知提出了一种新的安全方法论:不是依赖于规则而是依赖于这些安全情报,快速、动态地去改变这些安全配置。这样才能防止这种低频、高速的攻击。

人才和分享是关键

和许多美好的设想一样,态势感知目前也面临着掣肘它施展拳脚的问题。

刘政平告诉记者,在概念提出早期,做不到态势感知的原因很多,比如垃圾数据、数据分析不力等;而在当下,面临的一个重要困境是,没有足够的数据分析师人才队伍。

“没有足够的网络和数据分析师,就没有办法去有效地建模、建立规则库。”刘政平介绍说,这个工作其实非常枯燥,美国采取的办法是专设数据分析师这一岗位,并给予很高的薪水,以让分析师多年如一日地静下心来做。

“在中国,做工程师好像不如做管理的,水平高的工程师最后都去做了管理,那他的经验怎么沉淀呢?”刘政平反问道,缺乏人才团队是很多安全厂商的困惑,亚信安全致力于在成都形成产学研一体化的格局,就意在形成人才梯队,然后才是挖网络安全这座金矿。

此外,态势感知作为一种体系,分享也非常关键。刘政平对记者说,有的安全厂商甫一上马,就想做“大而全”,从数据收集到情报分析、交叉分析想要一口气全做完。“这是不现实的,大家各有专长、各显神通才是把态势感知做好的最佳态度。”

基于此,刘政平认为,“态势感知这种事情就适合政府立项去做,才能推动厂商去互相共享”。

“态势感知是一种合作的生产,一般用户是推动不了的。”他说,现在可行的思路是各做各的专业,共同做生态,而不是做封闭式的、大而全的厂商。

平安城市的构建

引入态势感知的理念和技术,未来的网络安全提供商将扮演怎样的角色?

刘政平以亚信安全为例讲道:“我们更像一个平台,将各个安全技术和方案厂商团结在一起,构成一个大的安全防护体系和网络安全生态,共同为需方提供服务。”他说,构建平安城市这种系统工程的各项技术不是哪家企业或机构能够全部拥有的,比较好的做法就是构建一个开放和共享的平台,形成体系。

搭好了态势感知技术体系的台子,“平安城市”的建设成为最大的期许。早在今年3月,亚信安全就与成都市政府签订战略合作协议,“共建信息安全公共服务平台”。

然而,刘政平指出,还需要两个要素才能真正推进平安城市的建设。

“首先一定要有政策上的支持才能建成平安城市。一方面,毕竟谁都不愿意把自己不好的方面暴露出来,没有一把手推动很难成功。所幸政府高层越来越关注城市网络安全的话题,从贵阳到成都,我们都感受到了来自决策层的重视。另一方面,政策性的支持能够尽快建成良好的平安城市建设示范,包括一地安全生态的打造。这种示范作用对于未来的推广很重要。”刘政平说。

其次就是要联合可靠的安全企业。刘政平解释说,态势感知没有技术上的沉淀不行,采集的数据是否有效、情报分析到不到位、安全策略是否满足要求等都要达标。“不能到最后,连个黑客都抓不到,那是不行的。”

药品标准将被修改 涉及药企须慎重

政策风

本报讯 近日,国家药典委员会发布公告称,拟对单磷酸阿糖腺苷和注射用单磷酸阿糖腺苷的国家标准进行修订。该标准适用于生产该品种的所有企业。国家食品药品监管总局(CFDA)的资料显示,今年以来,CFDA已经两次就注射用单磷酸阿糖腺苷安全用药问题发了通知。

今年3月份,CFDA发布通知对注射用单磷酸阿糖腺苷的说明书进行修订,增加了9大不良反应,同时在儿童用药里面特别强调,目前尚无儿童应用本品的系统研究资料,建议儿童使用时权衡利弊。4月,国家食药监总局发布第70期《药品不良反应信息通报》,提示关注注射用单磷酸阿糖腺苷安全风险。

单磷酸阿糖腺苷是一种人工合成的腺嘌呤核苷类抗病毒药,其药理作用是与病毒的脱氧核糖核酸聚合酶结合,使其活性降低而抑制DNA合成,临床用于治疗疱疹病毒感染所致的口炎、皮炎、脑炎及巨细胞病毒感染。监测结果显示,注射用单磷酸阿糖腺苷不良反应报告数量近年来呈快速增长趋势,严重不良反应报告较多,超适应症用药现象比较突出。

国家药品不良反应病例报告数据库中有关注射用单磷酸阿糖腺苷的严重不良反应报告占总报告数的5.05%,14岁以下儿童不良反应的报告约占80%。

CFDA的信息显示,单磷酸阿糖腺苷(含注射剂)共有47条批文,对于部分药企来说,该药甚至占据其整体销售的很大一部分份额。CFDA虽然说是加强严管,但是,并不是说这个药就不能再用了,只是加强药品在安全性方面的监管,提醒临床用药必须更加注意安全用药,以及给药期间密切观察患者。在CFDA没有下令该产品退市之前,此产品仍可使用。

但是,对于产业来说,这给企业和药品经营人员最大的提醒是,药品的安全被放在了前所未有的地位,药品安全将是影响产品销售的关键。

而此事件给企业另一提醒是,对待药品超适应症使用,如果引起质量安全问题,一定要慎重再慎重,切勿为了市场,而不顾产品安全,未来这对产品也可能是致命的。以注射用单磷酸阿糖腺苷为例,它在我国批准的适应症为“用于治疗疱疹病毒感染所致的口炎、皮炎、脑炎及巨细胞病毒感染”,监测数据显示该品种存在超适应症用药现象,约占总报告数的79.98%,如用于支气管炎、肺炎、呼吸道感染、扁桃体炎等。

对于医药市场来说,未来真正能够在市场存活的,只有真正有作用的、安全可靠并且能够有及时并完善的临床信息反馈的产品。 **(陶朵朵)**

酷技术

图片来源:百度图片

生物机器人颠覆机器人定义

机器人,顾名思义,是可以执行任务的机器装置。然而,随着其承担的实验室之外的角色越来越多,传统机器人的刚性系统与其周遭的人类和环境互不兼容,安全隐患也越来越大。

对此,科学家们期望通过增添生物元素解决该问题,比如在传统制动器中增加气动人工肌肉或弹簧来增加缓冲力度。然而,国外新兴起的一股将机器人技术与(生物)组织工程学相结合的科研潮流,则提出了另一种解决方案,即研发由活体肌肉组织或细胞驱动的机器人,学名“生物合成机器人”。

这种机器人的制动器为活体细胞,细胞在受到光或电刺激后,发生收缩带动躯体弯曲,以完成相关动作或移动。它可像动物那样柔软地四处行动,与传统机器人相比,它对人和环境来说十分安全。因此,比其他高功率重量比的制动器更安全。此外,生物合成机器人的燃料来源仅是周围介质中的养分。

近日,美国哈佛大学生物工程和应用科学部门推出了全球首个生物合成机器人——“机器鳐鱼”。该团队通过对鳐鱼的生理机能进行逆向工程,创造出了长16毫米、重10克的微型机器人,看上去就像是一个透明硬币和一个尾巴的组合。

该团队首先使用一层透明的弹性聚合物作为主干部分,将大鼠心脏细胞以蛇形图案均匀分布在表面,再对细胞进行基因编码,使其对特定的蓝色闪光产生反应;用黄金制成支撑骨架,因为黄金对附着其上的细胞无抑制作用。

为供养“机器鳐鱼”中的活体细胞,研究人员把它放进充满糖的生理盐水中,并以蓝色的光脉冲对其电击。

为更好地控制细胞力量,科研人员使用了细胞图案化技术(微图形化技术),即在细胞依附的骨架上标出或印上微尺度线条。细胞沿线条整齐排列,这些线能随着细胞的成长指导它们。

此外,研究人员还可以通过改变光的频率来控制机器鳐鱼的移动方向,因“鱼身”两侧的细胞所响应的光的频率各不相同,如果以某一特定频率的光照射“鱼身”,那么只有一侧的细胞会产生收缩,以此完成转向动作,避开障碍物。

虽然生物合成机器人领域的起步令人十分兴奋,但距其能走出实验室还有很多的工作要做。 **(陶朵朵整理)**

高分三号 核心在手不求人

■潘晨

8月25日,高分三号卫星成像的首张图片正式发布。国家海洋局、气象局等用户纷纷称赞这些图像“震撼”、“质量非常好”。据悉,高分三号卫星的图像质量指标均达到国际先进水平,为卫星图像在各行业领域的应用奠定了坚实的基础。这标志着我国低轨道合成孔径雷达(SAR)卫星研制技术实现了重大突破,从此,我国民用天基高分辨率合成孔径雷达图像打破了全进口的现状,做到了核心在手。

攻克50多项重大关键技术 我国空间技术的又一瑰宝

为研制世界上性能最先进的C频段多极化合成孔径雷达卫星,卫星总体单位航天科技集团公司五院(以下简称“五院”)的科研人员通过技术创新,攻克了50多项重大关键技术,不仅实现了我国低地球轨道长寿命、高分辨率合成孔径雷达卫星研制技术的重大跨越,还将在引领我国民用长寿命高分辨率微波遥感卫星应用方面,起到重要的示范作用。

合成孔径雷达卫星由于不受光照、云层和天气的约束与影响,可以全天候、全天时工作,且具有对地下物体的穿透能力,解决了光学遥感观测不到或观测不足的问题,因此,一经问世,就备受追捧,成为航天大国竞相逐鹿的领域。我国研制的海洋二号、环境一号C合成孔径雷达卫星在应用上取得了极大的成功,但随着资源调查、减灾救灾、环境保护等众多领域需求的激增,研制性能更为先进、多用途的合成孔径雷达卫星,成为加快我国信息化建设的当务之急。

为此,五院的研制团队在系统设计上开展了大量的优化工作,先后攻克了低轨道卫星长寿命高可靠设计、分析及验证技术,大挠性高精度高稳定卫星控制技术,高品质万瓦级脉冲大功率电源及多母线供电技术,卫星机电热一体化、数字化三维协同设计及制造技术,陆海兼容多模式多极化成像技术等为代表的50多项关键技术,多项技术填补了国内和国际空白。

这些关键技术的突破,不仅实现了我国低地球轨道长寿命、高分辨率合成孔径雷达卫星研制技术“里程碑”式的重大跨越,还将极大地推动我国卫星工程的设计和研制技术的发展。“可以说,高分三号卫星的发射和应用,把我国高分系统建设由可见光、热红外、远红外带入到微波辐射区,迎来了卫星微波遥感应用的新时代”,高分三号卫星总指挥兼总师张庆君如是说。

实现微波图像数据自主 国家信息安全在握

高分三号卫星的问世,为国人用特殊的眼光审视地球提供了新手段,开辟了微波遥感应用的新境界。此前,我国民用合成孔径雷达卫星图像数据均为进口,不仅价格昂贵,且有时在紧急时刻不能很好地在第一时间获取数据。国内的用户都非常迫切希望高分三号卫星尽早发挥作用。高分三号卫星工程的用户涵盖了国内各类应用部门,各行业也迫切需要高分三号卫星工程提供的高质量连续稳定的合成孔径雷达图像,以替代目前大量进口的国外卫星数据。

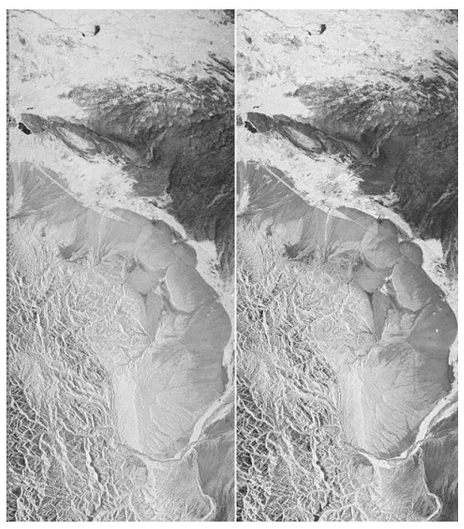
从本次发布的图像来看,高分三号卫星不辱使命,实现了连续、高质量、高精度对地观测。这颗卫星后续将源源不断地为祖国提供可靠、稳定的高分辨率微波图像数据,彻底结束了我国微波遥感数据图像长期依靠外国的历史,为建立我国独立自主的微波遥感数据系统,维护国家信息安全提供了可靠的保证。

发展前景广阔 期待来日飒爽英姿

作为一颗“百姓星”,高分三号卫星将履行以航天技术发展服务社会、造福人类的神圣使命。

高分三号卫星的用户包括国家海洋局、民政部、水利部、中国气象局以及十几个行业,其获取的信息在海洋观测、水利应用、灾害监测、环境监测等方面具有独特的优势,应用领域十分广泛。比如,通过高分三号卫星提供的可靠、稳定的高分辨率微波遥感图像,可以提高我国海洋环境灾害监测与预报能力,增强我国近海海域管理和环境保护的能力;可以为减灾备灾、应急救灾、恢复重建提供多层次、立体动态信息,加快灾害监测与评估进程,增强灾害的快速反应能力,对防灾救灾工作提供有力保障;可以进行台风、风暴潮、泥石流、山体滑坡等自然灾害监测预测,提高抵御自然灾害的能力。“在出现地震、滑坡、洪涝等自然灾害时,往往伴随恶劣的气象条件,并且要求快速响应提供灾区第一手图像信息,这个时候,类似高分三号的微波成像卫星往往发挥更大的作用”,高分三号卫星工程总师徐福祥说。

面对广阔的发展空间,五院专家呼吁,在强化高分三号卫星应用的同时,要坚持用研结合,加大投入,强化技术储备,加快新型功能更强合成孔径雷达卫星的研制,以保持在该领域的国际先进地位。此外,要着眼于多领域应用的迫切需要,构筑星座编队、多星组网的雷达卫星系统,为应用提供更为连续、丰富的信息源。



高分三号卫星拍摄的喀什地区影像。