

基于仿生机理的内生安全防御体系研究

胡爱群^{1,2}, 方兰婷^{1,2}, 李涛^{1,2}

(1. 东南大学网络空间安全学院, 江苏 南京 210096;

2. 紫金山实验室, 江苏 南京 211100)

摘要: 针对防火墙、入侵检测、防病毒等外壳式防御技术来不及检测、分析和过滤恶意流量, 防御机制没有与网络设备的安全状态关联, 导致安全效能低的问题, 提出一种基于仿生机理的内生安全防御体系。模仿生物体的高效安全防御机理, 在设计和建造信息系统时, 将巨量安全机制部署进入网络的每一个安全部件中, 通过网络互联将所有节点中的安全组件关联在一起, 对网络进行全面、深度的安全态势感知和防御, 并通过人工智能“大脑”不断地自主学习和演进, 提升发现未知威胁和自动处理威胁的能力。通过构建全新的内生安全防御体系, 将安全体系和信息系统高度融合, 能够解决现有信息系统防御效率低、无法处理高速率数据、不能应对未知威胁等问题, 使网络具有“与生俱来、自主成长”的安全防御能力, 满足“业务高可用、安全高效率”的信息系统发展需求。

关键词: 内生安全; 防御机制; 仿生安全; 自主学习

中图分类号: TP309.1

文献标识码: A

doi: 10.11959/j.issn.2096-109x.2021002

Research on bionic mechanism based endogenous security defense system

HU Aiqun^{1,2}, FANG Lanting^{1,2}, LI Tao^{1,2}

1. School of Cyber Science and Engineering, Southeast University, Nanjing 210096, China

2. Purple Mountain Laboratories, Nanjing 211100, China

Abstract: Shell-based security defense technologies such as firewall, intrusion detection and anti-virus cannot be updated in a timely fashion upon identification of attacks. The security defense mechanism is not associated with the security status of network devices, resulting in low security performance. To solve the above problems, an endogenous security defense system based on the bionic security mechanism was proposed. Firstly, imitating the security defense mechanism of the organism, the endogenous security system integrated the security component with each other at the construction process. Secondly, the endogenous security associates all security components through

收稿日期: 2020-05-08; 修回日期: 2020-07-03

通信作者: 方兰婷, 101012508@seu.edu.cn

基金项目: 国家自然科学基金(6162520); 至善青年学者支持计划

Foundation Items: The National Natural Science Foundation of China (6162520), Youth Scholar Program of SEU

论文引用格式: 胡爱群, 方兰婷, 李涛. 基于仿生机理的内生安全防御体系研究[J]. 网络与信息安全学报, 2021, 7(1): 11-19.
HU A Q, FANG L T, LI T. Research on bionic mechanism based endogenous security defense system[J]. Chinese Journal of Network and Information Security, 2021, 7(1): 11-19.

network interconnection, and proposed a defense in depth and comprehensive approach to increase the security of a system. Finally, through the self-learning, endogenous security's ability of threat detection was continuous enhanced. By integrating the security system and information system, an endogenous security defense system was constructed. The endogenous security defense system can handle the challenges such as low defensive efficiency ratio, high-speed data processing, and unknown threats detection. The endogenous security system is an efficient security defense system of "innate growth and independent growth". It meets the development needs of information systems with "high availability, security and high efficiency".

Keywords: endogenous security, defense mechanism, bionic security, independent learning

1 引言

随着 5G 无线网络进入商用阶段, 5G 不仅在数据传输速率、连接数密度、端到端时延、峰值速率和移动性等关键性能上比前几代移动通信系统更加丰富, 而且能为实现海量设备互联和差异性服务场景提供技术支持。同时, 下一代网络的广泛运用, 各类宽带、移动业务蓬勃发展, 应用类型日益精细区分, 信息系统规模不断扩大。5G 和下一代网络的发展, 带来了更多的安全问题, 这为内生安全防御机理提供了验证和实践的机遇。

1.1 外壳式防御无法适应网速和应用的高速发展

信息系统的安全性将对包括实体经济在内的社会、经济领域的安全造成重大影响。未来信息系统将为大量垂直行业服务, 如 AR/VR、远程驾驶、无线机器人、远程医疗、大视频、无人机、工业互联网等。信息系统灵活、高效、融合、开放的特性使创新业务在交通、工业等行业快速融合, 使垂直行业的应用更加多样化, 孕育新兴信息产品和服务, 创新行业应用, 重塑产业发展模式。因此, 信息系统在保证安全性的同时, 需要将信息快速有效地进行传输, 避免恶意流量、恶意软件、非法接入等带来的危害。

如图 1 所示, 现有的信息系统通过在网络节点部署防火墙、防病毒软件、入侵检测系统来保障网络数据传输的安全性, 这是一种“外壳式”防御方法。

防火墙是设置在用户网络和外界之间的一道屏障, 防止不可预测的、潜在的破坏侵入用户网络。防火墙在开放和封闭的界面上构造一个保护层, 属于内部范围的业务, 依照协议在授权许可下进行; 外部对内部网络的访问受到防火墙的限制。

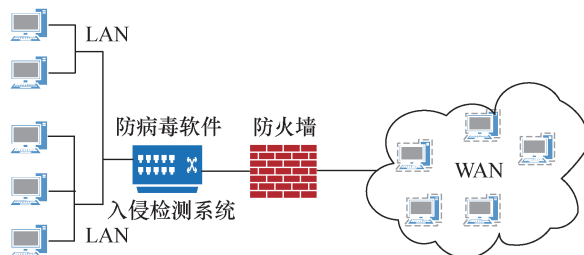


图 1 外壳式防御系统
Figure 1 Shell-based security system

防病毒软件通过扫描过滤技术, 完成病毒查杀工作。例如, 在防病毒软件中植入文件扫描过滤技术, 防范有病毒的文件, 或者在网络网关上配置反病毒软件, 过滤含病毒的网站。

入侵检测系统是一个动态的防御系统, 它是对防火墙和防病毒软件的补充。入侵检测系统能通过分析、审计记录, 识别系统中任何不应该发生的活动, 并采取相应的措施报告并制止入侵活动。入侵检测系统的主要功能包括: 监测并分析用户和系统的活动情况; 检查系统的配置和漏洞; 评估系统关键资源和数据文件的完整性; 识别已知的攻击行为; 统计分析异常行为; 管理操作系统日志, 并识别违反安全策略的用户活动。

然而, 5G 移动网络架构日趋复杂, 数据量呈指数级增长, 数据来源更加丰富, 内容更为细化, 网络数据分析的维度更广泛。同时, 随着移动终端设备性能的增长, 数据源发送速率更快, 对安全信息采集的速度要求越来越高, 漏洞日益增多, 影响更加广泛。这些变化使外壳式防御体系面临问题: ① 防火墙来不及深度过滤; ② 入侵检测系统来不及检测入侵; ③ 防病毒软件来不及发现病毒。这些问题导致了信息网络和信息安全“两张皮”的外壳式防御方法无法保证逐渐一体

化的巨流量信息网络安全。因此, 需要提出一种全新的安全防御体系, 将安全体系和信息系统高度融合, 使信息系统在安全防御过程中, 既能有效地避开威胁, 又不影响正常的信息传输过程, 同时可以不断调整和提高应对威胁的能力。

1.2 安全防御成为信息系统的负担和应用发展的障碍

随着信息系统规模的扩大, 网络上的数据正呈爆炸式的增长速度。大数据时代的到来不仅为传统安全问题提供了新的分析思路, 也给现有的数据分析理论和方法带来了新需求和新问题。其中, 数据的大体量、高维度使早期的集中式防御方法面临高存储、高计算复杂度等挑战。

近年来, 随着网络分布式计算的发展, 安全防御研究思路逐渐从集中式单点检测向分布式检测方案转变^[1-2]。例如, 文献[3]通过分离数据与控制平台为网络提供高度开放性和可编程性, 针对已有工作中 SDN 主动防御框架缺乏考虑网络瓶颈的问题, 提出了分布式欺骗防御系统。文献[4]提出了在实时环境中检测分布式拒绝服务(DDoS, distributed denial of service)攻击的方法, 通过人工神经网络(ANN)算法区分 DDoS 攻击流量与真实流量的特定特征。文献[5]提出了一种完全分布式的框架, 用于研究面对多个攻击者发起的分布式拒绝服务攻击时, 多代理系统的协同行为。总体而言, 相对于集中式的单点检测, 分布式的混合型机制能够利用位于网络中不同位置的节点进行全面的攻击检测和响应, 从而尽早确认攻击流量并在源端进行防御。

在构建分布式的混合型防御体系过程中, 其中一个需要解决的问题是如何让安全防御不成为整个通信系统的负担。在现有的分布式防御体系中, 所有传播的信息必须先通过安全检测系统。当数据体量很大时, 安全检测系统严重降低了流量传输的速度。在安全检测速度跟不上流量传输速率的情况下, 实际应用中会通过简化安全防御策略来提高信息传输速度, 进而导致系统安全防御效果严重下降。例如, 现有的入侵检测系统通常部署在网络的主干节点, 对

吞吐性能要求高, 大量的应用级检测、过滤计算造成了严重的计算瓶颈, 因此很多研究机构只是进行较低层次的数据包分析, 限制了系统的使用效果。

除了不让安全防御成为系统负担, 另一个待解决的问题是如何创建联动机制, 综合分析和处理各个安全状态采集器之间的信息。随着信息载体类型和网络互联互通方式的增多, 客观上为攻击者提供了更多的潜在入口和可利用途径, 传统的防御体系没有联动机制, 难以处理每个采集器之间的关联关系。例如, 防火墙大多采用“一刀切”的防御方法, 对所有可疑数据包进行拦截, 缺少对信息系统自身的分析和联动, 而对系统不构成威胁的数据包进行分析和拦截进一步影响了效率。因此, 需要提出一种联动处理方法, 在不影响信息系统速度的情况下综合分析所有的信息。

2 相关概念

2.1 生物神经系统

生物神经系统给安全防御研究提供了新思路。首先, 生物在面临外部威胁时, 往往能够产生合理的、适度的反应。例如, 当人体的手接触到蜡烛的火焰时, 人往往只会移开手, 而不是反应过度地从此不再接触火。这是一种基于自身认识对外部攻击的适度响应。其次, 生物体内拥有的强大免疫系统能够抵御病毒的内部入侵, 这是一种内部攻击发生后的免疫行为。最后, 生物针对未知的威胁, 通过自我学习, 逐渐地具备防备此类威胁的能力。例如, 婴儿可以通过对外界的不断感知, 学习走路, 防止摔倒, 自身的免疫力也能够通过“免疫记忆”的方式逐渐提高, 这是一种“自我生长”的能力。

生物的这种安全防御能力是与生物自身高度融合的, 是一种“内生”的安全机制, 这种能力在系统的目标、结构及工作模式上与信息系统安全防御具有高度相似性, 给研究者极大的启示。因此, 在信息系统中构造类似于生物防御系统的内生安全机制是理想的主动防御措施, 引起了网络安全研究者的重视。总体来看, 目前内生安全的研究主要包括 3 部分: 计算机免疫、拟态安全和智能安全。

Forrest 等^[6]提出了计算机系统中的类似生物免

疫的模型,并在计算机上建立了一个人工免疫系统。在这个模型中,每台主机是一个检测节点,整个系统由分布在网络中处于监听状态的一组主机构成。此外, Kim 和 Dasgupta 两个研究小组分别开展了基于阴性选择模型的入侵检测系统的研究,提出了各自的抗体和抗原匹配算子并研究了检测器的生成算法^[7-8]。Luo 等借鉴生物免疫系统的抗体生长和成熟机制^[9-10],提出并解决了检测器自适应生成问题、检测器分配问题。周建国等^[11]采用人工免疫模型建立了面向广播式局域网的入侵检测模型的框架。但由于信息系统现有体系架构的限制,构建的免疫防御的机制缺乏应用环境的支撑,通常应用在检测系统内部的病毒攻击方面。

生物规避风险的一种行为是通过伪装躲避攻击,这就是“拟态现象”,即一种生物在色彩、纹理和形状等特征上模拟另一种生物或环境,从而使一方或双方受益的生态适应现象^[12]。一些研究者根据拟态现象提出相应的安全防御方法,代表性的方法就是郭江兴提出的“拟态防御”^[13],该方法基于生物的拟态现象,提出了一种通过类似拟态伪装的方式进行主动隐匿,较大程度上增加了攻击的难度。拟态防御旨在隐藏受保护目标,使攻击行为难以实施^[14-15]。

智能安全是使用人工智能的方法对威胁进行分析,具有发现未知威胁的效果。近年来,人工智能在网络安全领域的应用初显端倪,从影响力和科技水平来看,人工智能的下一个热点会是网络安全,人工智能将是下一代安全解决方案的核心^[16-17]。MIT 的 CSAIL 实验室与初创公司 PatternEX 共同开发的端到端系统“AI2”,可以不断学习来自安全分析员的反馈,从而对新发生的事件进行预测,其准确率是类似的自动化网络攻击检测系统的 2.92 倍,误报率是同类的安全解决方案的 1/6^[18-19]。一些知名安全厂商开始了从使用以签名为基础的反病毒和反恶意软件产品到采用不再依赖现有恶意软件定义的机器学习模式来检测威胁的转变。

2.2 网络空间安全

敌对势力的破坏、黑客攻击、恶意软件侵扰、利用计算机犯罪、隐私泄露等,对信息安全构成了极大威胁。除此之外,科学技术的进步对信息

安全提出新的挑战。由于量子 DNA 计算机具有并行性,从而使许多现有公钥密码在量子 DNA 计算机环境下不再安全。因此,网络空间安全的形势是严峻的。

生物的防御系统同时处理大量的攻击信息,不会影响到生物的其他功能。因此,需要基于生物防御系统研究出一种不影响信息系统其他功能的安全防御方法。

生物的神经系统神秘而复杂,研究根据已知的神经科学知识,建立网络安全防御机制是一个复杂的问题。生物的安全防御系统具有各个结构和功能相互合作又各不影响的特性,理想的网络安全防御体系也应该具有这样的特性。若要实现这一特性,需要实现以下功能:① 安全和功能组件高度融合;② 大脑为安全风险决策;③ 整体协作达到安全。这种基于生物神经系统建立的安全防御机制叫作内生安全。

3 内生安全体系

传统的安全防御体系通常是在反恶意软件、网络流量异常检测、网络安全运营和系统安全性评估等具体领域孤立地开展。智能安全是使用人工智能的方法对威胁进行分析,具有发现未知威胁的效果^[16-17]。

内生安全从仿生学的角度,构建基于生物神经系统的信息系统内生安全体系。和现有的智能安全研究的区别是:内生安全将人体仿生系统、免疫、人工智能与 5G 移动通信网络进行融合,参考人体神经系统分布式感知的特性布置巨量感知器,实时监测系统各部分变化,使用人工智能的方法构造类人脑的安全中心,通过汇总的信息做出决策,从而对外部入侵进行合理反制,对内部入侵进行免疫式防御。仿生体现在感知网络的部署、类人脑的学习和决策、外部入侵的适度反制上,免疫体现在对内部入侵的标记和防御上,是一种基于仿生免疫的内生安全机制。根据仿生免疫的思想,攻克构建与信息系统高度融合的仿生免疫体系,设计分布式细粒度威胁感知与反制机制,设计与信息系统并行融合的多层传输网络,建立不可复制的接入控制机制,使用人工智能的方法构建具有学习、处理、决策能力的安全中心

等基础理论问题。在 5G 网络中部署感知、响应、免疫、安全中心这些关键安全部件，通过人工智能“大脑”的自主学习和演进，通过感知、判断、对抗和反制、自主生长等生物与生俱来的自主反应能力，形成分布式细粒度威胁感知与反制、多层安全防御网络、类脑安全控制和自主进化和决策等安全机理。建立“与生俱来、自主成长”的安全防护体系，主动应对信息系统面临的安全威胁，打造全新的安全体系架构。

3.1 目标与路线

内生安全旨在解决由于网络的快速发展和信息系统规模的扩大使安全防御系统来不及检测威胁的问题和无法处理未知威胁的问题。即在设计、建造未来的信息通信系统时，把与安全相关的要素部署进入信息系统的每一个环节中，通过人工智能“大脑”的自主学习和演进，主动应对信息系统面临的安全威胁，形成系统级的安全防护体系，且不会显著影响通信系统的业务可用性。使内生安全系统具有以下能力。

- 1) 感知能力，能够感知局部和整体运行环境的安全性，获取相关信息。
- 2) 判断能力，能够根据感知到的信息进行分析、计算与判断。
- 3) 对抗和反制能力，能够消灭威胁，甚至可以反过来攻击对方的防御系统。
- 4) 自主生长能力，能够通过与运行环境的交互作用，使自己能够适应环境变化，应对安全事件。通过体系模型的研究提出适用于信息网络的内生安全架构与内生安全机制，并对各部分的接口进行标准化规范。

3.2 基本概念

图 2 给出了内生安全防御体系的系统框图，内生安全通过在各类安全功能之间建立桥梁，使彼此能够交互信息，创建一个高度智能化的安全体系，自动化应对安全事件。以信息系统为对象，研究覆盖终端、基站、核心网、应用系统在内的仿生免疫体系整体架构，提出各部分功能部件融入安全功能的标准，在不降低系统运行效率的情况下实现系统的内生安全防护，使信息系统在安全上具有感知能力、判断能力、对抗和反制能力、自主生长能力。

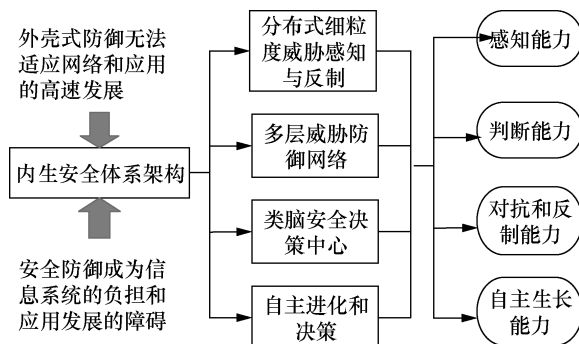


图 2 内生安全防御体系
Figure 2 Endogenous security defense system

面向信息系统，以功能部件为基本单位，研究和部署大量类人体神经系统的分布式的细粒度威胁感知器和传导机制，实时全面掌握系统的安全态势；在安全部件中增加安全反制防御部分，把威胁或破坏消灭在局部，而不至于扩散到系统。在感知与反制基础上，建立各种机制之间的关联和分析方法，构建高度并行融合的安全事件多层传输网络，形成多层的安全神经网络，提高安全决策的效率；研究和设计仿生免疫安全体系所需的网络协议，满足免冲突、安全性、高效性等要求。

研究基于类脑智能的信息系统安全决策机制，构建智能安全中心，该安全中心可以并行高效地处理多模态海量数据，自主分析数据之间的关联性、决策和自学习进化，判断事件的安全本质特性并及时做出反馈，从而根据发现的风险产生对系统的控制决策，并将控制命令传达给系统中的多个模块联动执行，实现系统风险最小化的信息网络高效防护，维护信息系统的整体安全性。

3.3 内生安全体系与模型

随着计算机网络规模和复杂性的不断增大，网络的脆弱性越来越强。面对网络攻击技术的不断革新，传统的安全技术显得“力不从心”。网络入侵不可避免，网络难免会遭受安全事件的损害从而存在安全风险。

人体面临各种威胁时，往往能够产生合理的、适度的反应。而现行的一些防火墙，往往会选择隔离此类威胁，从而大大影响了用户体验。此外，人体针对未知的威胁，会通过自我学习，逐渐地具备防备此类威胁的能力。例如，婴儿可以通过

对外界的不断感知,而逐渐提高自我的免疫力。因此,研究人体对外界威胁的智能反应对信息系统安全具有重要意义,在人体防御过程中,既能有效地避开威胁,又不会影响正常的日常生活,同时可以不断调整和提高应对威胁的能力。

通过参考相关生物学文献发现,正是遍布全身的神经元为人体提供了这样的能力。神经元通过对周围环境的感知以及分级的神经系统,为大脑做出合适的判决提供了源源不断的信息,如温度、表面粗糙度、湿度等。神经系统(nervous system)是机体内部对生理功能活动的调节起主导作用的系统,主要由神经组织组成,分为中枢神经系统和周围神经系统两大部分。中枢神经系统包括脑和脊髓,周围神经系统包括脑神经和脊神经。传感器既用于实现各种功能,又用来实现安全目的。

除此之外,人体还具有一套免疫系统,免疫系统具有免疫监视、防御、调控的作用,包括先天免疫和获得性免疫。免疫系统包含免疫器官、免疫细胞、免疫分子。通过免疫系统能够识别入侵(非己);识别恶意程序(清除肿瘤);保护自身安全(自身功能的稳定)。

上述人体安全系统主要特征在于遍布系统的海量传感器、综合分析处理中心、遍布系统的联动的应对处理模块。将人体的神经网络进行抽象,与信息系统进行类比,可以得到如图 3 所示的抽象类比结构,该结构主要包含 3 部分。

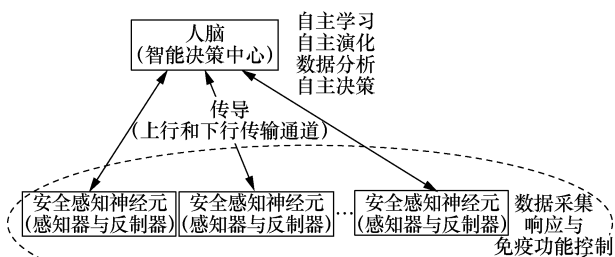


图 3 人体神经系统与仿生免疫抽象类比
Figure 3 Comparison between human nervous system and bionic immunity

(1)安全感知神经元是安全架构的底层组织,包含安全传感和防护反制功能,能够感知安全相关事件数据,将事件反馈并进行防护机制的实施。安全传感包括网络正常行为的描绘、数据包深度检测、可疑活动的偏离行为、前端设备的运行情

况等,将数据进行实时上报。防护功能包含传统的安全机制,如加密、访问控制、阻断等;也包含一些功能性措施,如降低负载、提高运行速度等。

(2)智能决策中心是安全架构的大脑,通过不断学习、自我完善,使安全防御的各个结构和功能相互合作又各不影响。通过类脑安全控制并行处理体系的数据,实现多任务整合、归纳和决策。通过自主进化决策对潜在的风险自主学习,实现安全性能的自我提升。智能决策中心具有整合、归纳和决策能力,对各部分神经元汇聚的数据进行分析,并根据已有的经验进行防护部署。对收集到的来自分布式前端设备的数据进行集中化处理,描绘出潜在的安全缺口。在数据分析的过程中采用先进的交叉数据规律逻辑分析,用于辨别基于多种类设备和多层信息逻辑的缺口和威胁。智能决策中心具有自学习和自适应能力,在已知的缺口上使用机器学习技术,实现前瞻性安全防护和异常行为辨别。根据已有的专家知识库提供设备异常行为的辨别方法,当可疑和可能的恶意活动发生时采取措施。在安全防护措施实施时,根据全网和全系统的运行情况进行核心任务防御机制的部署,确保核心功能的稳定运行。

(3)上行和下行传输通道,包含安全数据汇集和策略分发的机制和协议,提供上下行通道数据防护协议,确保采集数据的快速、完整上报和下行防护策略的正确配置。

3.4 满足巨量感知、响应与免疫的多层高效安全机制

传统的入侵检测、防火墙、病毒检测等技术属于被动防御手段^[20],只能对系统局部进行检测,获取的信息之间缺乏关联。近年来,网络安全态势感知技术逐渐引起研究人员的兴趣^[21-22]。网络态势感知技术可以从全局的角度识别、理解和分析威胁时间和空间环境中的元素,把握网络整体安全状况及预测未来变化趋势。这类方法从大量数据中辨识网络中的攻击活动,融合这些信息对网络的安全态势进行实时评估和监控,并进行有效响应。然而,由于网络攻击的随机性和不确定性,网络安全态势变化成为一个复杂的非线性

性过程, 传统的态势感知模型无法依据网络环境威胁的变化主动调整整个系统的防御策略, 同时缺乏自适应性, 无法识别未知攻击, 不能防范日益严重的网络安全威胁。

生物防御系统是一个高度并行、分布、自适应、自组织的系统, 具有很强的学习、识别、记忆和特征提取能力, 具有强大的信息处理能力。信息系统的内生安全系统希望从生物防御系统的运行机制中获取灵感, 构建高度并行融合的多层安全防御网络, 用于解决网络空间安全的实际问题。

生物防御系统具有以下威胁防御能力: 在攻击发生前规避风险; 在攻击发生后免疫风险。为了在信息系统中实现类似的安全防御能力, 巨量感知、响应与免疫的多层高效安全机制的研究重点包括两方面。

(1) 以功能部件为基本单位, 研究和部署大量类人体神经系统的分布式的细粒度威胁感知器和传导机制, 实时全面掌握系统的安全态势; 在安全部件中增加安全反制防御部分, 把威胁或破坏消灭在局部, 而不至于扩散到系统。部署反制系统, 在遇到威胁后, 反制对方的攻击系统。

(2) 在感知与反制基础上, 建立各种机制之间的关联和分析方法, 构建高度并行融合的安全事件多层传输网络, 形成多层的安全神经网络, 提高安全决策的效率。研究和设计仿生免疫安全体系所需的网络协议, 满足免冲突、安全性、高效性等要求。

3.5 类脑安全控制中心

受脑信息处理机制启发, 借鉴脑神经机制和认知行为机制, 发展类脑智能已成为近年来人工智能与计算科学领域的研究热点^[23]。已有的人工智能算法大多被设计用来执行特定任务, 需要大量的数据集和强大的运算能力, 才能获得执行任务的能力。相较而言, 人脑更擅长处理多任务, 快速实现多感觉整合、归纳以及决策, 而且只需要非常低的能耗。

美国国家科技委员会于 2016 年 10 月发布了题为“为人工智能的未来做好准备”的报告^[24], 划定美国人工智能发展路线和策略, 报告用专门

的章节阐述“人工智能和网络安全”, 描绘了当前和未来人工智能在网络安全领域的美好蓝图。英国也高度重视智能网络攻防的研究, 并开展了人工智能应用于军事网络防御的相关演习。此外, 欧盟将“人脑工程计划”列入未来新兴旗舰技术项目; 日本、韩国、加拿大等先后发布大脑发展战略和共识; 艾伦研究所、谷歌公司、微软公司等研究机构和企业, 纷纷加入该项目。

我国神经科学与人工智能界已经初步提出“脑科学和类脑研究”和“人工智能 2.0”计划^[25-26]概念。该脑科学和类脑研究以“一体两翼”为基础操作框架, 关注脑认知科学的基础知识、神经精神性疾病的诊断与干预、类脑研究^[27]。“人工智能 2.0”涉及大数据智能、群体智能、跨媒体智能、人机混合增强智能、自主智能系统等领域。类脑研究是内生安全体系的研究重点, 内生安全中类脑安全控制技术的研究重点包括 3 方面。

(1) 研究基于类脑智能的网络安全控制技术, 维护系统的整体安全性, 可以并行高效地处理海量数据, 分析数据之间的关联性, 判断事件的安全性并及时做出反馈。

(2) 在重视类脑智能的网络安全控制技术前沿理论研究的基础上, 应积极开展计算神经科学研究, 充分利用神经科学研究成果, 挖掘人脑智能机制, 建立类脑智能新理论, 开发类脑人工智能算法和新模型。一方面, 类脑人工智能的技术突破, 需要有新理论、新算法、新模型的支撑; 另一方面, 加强人工智能技术与产品的研发、应用和产业化发展, 可以反过来助力神经科学研究与创新。

(3) 将人工智能的自我学习过程与人类已经积累的大量高度结构化的安全知识相融合, 使内生安全体系拥有高度感知、逻辑推理、抽象思维等高级认知功能。

3.6 自主进化和决策

学习与记忆是人类和动物认识世界的基础之一, 理解人类如何在不确定的环境中做出适应性反应, 是基于人类防御系统构建内生安全体系的重要理论基础。

传统的安全防御系统的方法是试图建立一个完全安全的系统。然而, 在实践中, 建立完全安

全的系统是不可能的。首先,设计和实现一个整体安全的系统相当困难。其次,现有的加密方法、访问控制和保护模型等本身存在一定问题。最后,安全系统会受到不可控因素的影响,如内部用户的攻击等。

既然建立完全安全的系统是不现实的,而且现有的安全技术措施具有各种不足。那么一个实用的方法是建立比较容易实现的安全系统,同时按照一定的安全策略建立相应的安全辅助系统,该系统能够在不影响现有系统工作及网络性能的前提下进行学习和自我完善,并为系统提供对内部和外部攻击以及误操作有效的保护手段。

人体防御系统具有良好的多样性、耐受性、免疫记忆、分布式并行处理、自组织、自学习、自适应和鲁棒性等特点。计算机系统的安全问题与人体防御系统所遇到的问题具有惊人的相似性,两者都是在不断变化的环境中维持系统的稳定性,这将为生物防御系统引入网络空间安全防护研究领域提供充分的理论依据。

安全资源的消耗无法应对当前海量的检测需求,因此需要在确保系统安全的情况下,解决安全防御带来的过量系统负担问题。利用模拟生物的自适应能力优化安全决策,实现去中心化或者部分去中心化的安全防护,降低消耗。在局部完成主要的安全感知和决策的工作,保证系统的运行效率,同时最小化安全风险,实现高效的信息网络防护体系。模拟人体防御系统的自我学习机制,不断提高安全系统的防御能力。自主进化和决策的研究重点包括以下 3 方面。

(1) 多模态感知整合研究,生物的大脑整合不同模态的感知信息从而做出最优化的判断,这是生物智能发展的重要基础,内生安全研究需要基于生物的整合判断的方式,通过整合不同模态的感知信息,用于解决网络空间系统中遇到的实际问题。

(2) 决策行为的研究,决策是从多种选项中挑选出结果的思维或认知过程,是生物在不确定的环境中做出的适应性反应,内生安全体系需要根据生物的决策行为做出对网络攻击事件的适应性反应。

(3) 学习与记忆机制,学习与记忆是人体认

识世界的基础之一,因此,内生安全应该以人体的学习与记忆为基础,开展自我进化的研究。

4 结束语

内生安全的体系参考人体神经系统分布式感知的特性布置巨量感知器,实时监测系统各部分变化,使用人工智能的方法构造类人脑的安全中心,通过汇总的信息做出决策,从而对外部入侵进行合理反制,对内部入侵进行免疫式防御。

内生安全体系的研究方向包括以下 3 方面:

① 满足巨量感知、响应与免疫的多层高效安全机制,主要研究如何部署大量分布式的细粒度威胁感知器、传导机制和安全反制防御机制,以及如何建立各种机制之间的关联和分析方法;② 类脑安全控制中心,主要研究基于类脑智能的网络安全控制技术、计算神经科学研究、融合人工智能的自我学习过程和人类已经积累的安全知识;③ 自主进化和决策,主要研究学习与记忆机制、决策行为的研究、多模态感知整合研究。

通过构建内生安全防御体系,最终能够解决现有通信网络防御效率低、无法处理高速率数据、不能应对未知威胁等问题,使安全体系和信息系统高度融合,安全体系可以主动应对信息系统面临的安全威胁,形成系统级的安全防护体系,且不会显著影响信息系统其他功能的可用性。

参考文献:

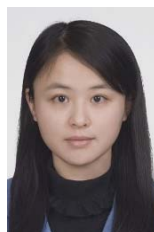
- [1] YAN Q, YU F R, GONG Q, et al. Software-defined networking (SDN) and distributed denial of service (DDoS) attacks in cloud computing environments: a survey, some research issues, and challenges[J]. IEEE Communications Surveys & Tutorials, 2015, 18(1): 602-622.
- [2] WANG K, DU M, MAHARJAN S, et al. Strategic honeypot game model for distributed denial of service attacks in the smart grid[J]. IEEE Transactions on Smart Grid, 2017, 8(5): 2474-2482.
- [3] 徐明迪, 高杨, 崔峰. 基于 SDN 的分布式欺骗防御系统[J]. 通信学报, 2018, 39(A2): 54-60.
XU M D, GAO Y, CUI F. Distributed deception defense system based on SDN[J]. Journal on Communications, 2018, 39(A2): 54-60.
- [4] SAIED A, OVERILL R E, RADZIK T. Detection of known and unknown DDoS attacks using artificial neural networks[J]. Neuro-computing, 2016, 172: 385-393.
- [5] XU W, HU G, HOD W, et al. Distributed secure cooperative control under denial-of-service attacks from multiple adversaries[J]. IEEE Transactions on Cybernetics, 2019: 1-10

- [6] FORREST S, HOFMEYR S A, SOMAYAJI A, et al. A sense of self for UNIX processes[C]//In Proceedings of the 1996 IEEE Symposium on Security and Privacy. 1996: 120-128.
- [7] GONZALEZ D. An immunogenetic approach to intrusion detection[R]. 2001.
- [8] BENTLEY K. The artificial immune model for network intrusion detection[C]//The 7th EUFIT'99. 1999.
- [9] LUO W J, ZHANG S H, LIANG W, et al. NIDS research advance based on artificial immunology[J]. Journal of University of Science and Technology of China, 2002, 22(5): 520-531.
- [10] BECK G, HABICHT G S. Immunity and the invertebrates[J]. Scientific American, 1996, 275(5): 60-66.
- [11] 周建国. 网络入侵检测的免疫学建模及其仿真研究[D]. 北京: 北京航空航天大学, 2002.
- ZHOU J G. Simulation and modeling of immunology network intrusion detection[D]. Beijing: Beijing University, 2002.
- [12] Mimic octopus. Wikipedia, the free encyclopedia[EB].
- [13] 邹江兴. 网络空间拟态防御研究[J]. 信息安全学报, 2016, 1(4): 1-10.
- WU J X. Research on cyber mimic defense[J]. Journal of Cyber Security, 2016, 1(4): 1-10.
- [14] HU H C, WU J X, WANG Z P, et al. Mimic defense: a designed-in cybersecurity defense framework[J]. IET Information Security, 2017, 12(3): 226-237.
- [15] HU H C, WANG Z P, CHENG G Z, et al. MNOS: a mimic network operating system for software defined networks[J]. IET Information Security, 2017, 11(6): 345-355.
- [16] BUCZAK A, GUVEN E. A survey of data mining and machine learning methods for cyber security intrusion detection[J]. IEEE Communications Surveys & Tutorials, 2015, 18(2): 1153-1176.
- [17] HAREL Y, GAL I B, ELOVICI Y. Cyber security and the role of intelligent systems in addressing its challenges[J]. ACM Transactions on Intelligent Systems and Technology. 2017, 8(4): 49.
- [18] DONG Y, HAN Q L. Guest editorial special issue on new trends in energy internet: artificial intelligence-based control, network security, and management[J]. IEEE Transactions on Systems, Man, and Cybernetics, 2019, 49(8): 1551-1553.
- [19] JESCHKE S, BRECHER C, SONG H B, et al. Industrial internet of things and cyber manufacturing systems[M]. Springer International Publishing, 2017: 3-19.
- [20] 张焕国, 韩文报, 来学嘉, 等. 网络空间安全综述[J]. 中国科学: 信息科学, 2016, 46(2): 125-164.
- ZHANG H G, HAN W B, LAI X J, et al. Cyber security overview[J]. Science China: Information Science, 2016, 46(2): 125-164.
- [21] VINCENT L, TANNER A, BLARER A. Gaining an edge in cyberspace with advanced situational awareness[J]. IEEE Security & Privacy, 2015, 13(2): 65-74.
- [22] 李艳, 王纯子, 黄光球, 等. 网络安全态势感知分析框架与实现方法比较[J]. 电子学报, 2019, 47(4): 927-945.
- LI Y, WANG C Z, HUANG G Q, et al. A survey of architecture and implementation method on cyber security situation awareness analysis[J]. Acta Electronica Sinica, 2019, 47(4): 927-945.
- [23] POO M M, DU J L, LP N Y, et al. China brain project: basic neuroscience, brain diseases, and brain-inspired computing[J]. Neuron, 2016, 92: 591-596.
- [24] BUNDY A. Review of preparing for the future of artificial intelligence[J]. AI and Society, 2017, 32(2): 285-287.
- [25] PAN Y H. Heading toward artificial intelligence 2. 0[J]. Engineering, 2016, 2(4): 409-413.
- [26] PAN Y H. Special issue on artificial intelligence 2. 0[J]. Frontiers of Information Technology & Electronic Engineering, 2017, 18: 1-2.
- [27] 蒲慕明, 徐波, 谭铁牛. 脑科学与类脑研究概述[J]. 中国科学院院刊, 2016, 31(7): 725-736.
- PU M M, XU B, TAN T N. Brain science and brain-inspired intelligence technology-an overview[J]. Bulletin of Chinese Academy of Sciences, 2016, 31(7): 725-736.

[作者简介]



胡爱群(1964—), 男, 江苏如皋人, 博士, 东南大学教授、博士生导师, 主要研究方向为网络与信息安全、移动通信安全技术。



方兰婷(1990—), 女, 安徽六安人, 博士, 东南大学讲师, 主要研究方向为内生安全技术、数据挖掘技术、人工智能技术。



李涛(1984—), 男, 江苏镇江人, 博士, 东南大学讲师, 主要研究方向为安全评估、移动终端防护。