DOI 10.15302/J-SSCAE-2023.06.007

从自卫到护卫：新时期网络安全保障体系构建与发展建议

田志宏[1]，方滨兴[1*]，廖清[2]，孙彦斌[1]，王晔[2]，杨旭[2]，冯纪元[2]

（1. 广州大学网络空间安全学院，广州 510006；2. 哈尔滨工业大学（深圳）计算机科学与技术学院，广东深圳 518055）

摘要：随着网络攻防技术的快速发展，网络安全保障体系面临诸多挑战，研究新型网络安全保障体系成为推进我国信息化发展的迫切需要，对进一步提升网络安全性、可用性具有重要意义。本文梳理了我国以“自卫模式”为主的网络安全保障体系的运行现状；分析了当前体系面临的“捕不全”“拦不住”“看不清”和“抓不住”四大安全问题；提出了以近身蜜点、前置蜜庭、网关蜜阵、外溢蜜洞的“四蜜”威胁感知体系为代表的“护卫模式”网络安全保障体系，包括纵深威胁感知的蜜点技术、攻击观测和判别的蜜庭技术、协同联动的蜜阵技术和网络威慑与攻击绘制的蜜洞技术等重点发展的技术任务，以及“蜜点”加持的网络安全保险产业任务。研究建议，探索“护卫模式”网络安全保障机制，全面提升国家网络安全防护水平；探索“护卫模式”安全防护技术研究和应用，实现新旧安全防护技术的融合统一；探索面向“护卫模式”的网络安全人才培养新模式，培育创新实践型网络人才，为新时期我国网络安全保障体系研究提供参考。

关键词：网络安全；保障体系；威胁攻击；主动防御；护卫模式

中图分类号：TP393　　**文献标识码：**A

Cybersecurity Assurance System in the New Era and Development Suggestions Thereof: From Self-Defense to Guard

Tian Zhihong[1], Fang Binxing[1*], Liao Qing[2], Sun Yanbin[1], Wang Ye[2], Yang Xu[2], Feng Jiyuan[2]

(1. Cyberspace Institute of Advanced Technology, Guangzhou University, Guangzhou 510006, China; 2. School of Computer Science and Technology, Harbin Institute of Technology (Shenzhen), Shenzhen 518055, Guangdong, China)

Abstract: The rapid development of network attack and defense technologies has posed various challenges to current cybersecurity assurance systems. Therefore, studying a new cybersecurity assurance system has become an urgent need to promote the development of information technologies and is of strategic significance for strengthening the network security and availability in China. This study summarizes the operation status of and major security challenges faced by China’s current cybersecurity guarantee system that features a self-defense mode. A cybersecurity guarantee system based on a guard mode and its key technical tasks are proposed. Specifically, the tasks include honey point technology based on deep threat perception, honey court technology based on attack observation and discrimination, honey matrix technology based on collaborative linkage, and honey hole technology based on attack deterrence and mapping. Furthermore, we propose the following suggestions: (1) exploring the cybersecurity assurance mechanisms based on the

收稿日期：2023-08-22；**修回日期：**2023-10-30

通讯作者：*方滨兴，广州大学网络空间安全学院教授，中国工程院院士，研究方向为网络空间安全；E-mail: fangbx@cae.cn

资助项目：中国工程院咨询项目“网络安全保障体系战略研究”(2022-JB-04)

本刊网址：www.engineering.org.cn/ch/journal/sscae

guard mode to comprehensively improving the cybersecurity protection level of China; (2) exploring the research and application of security protection technologies based on the guard mode and achieving the integration of existing and new security protection technologies; (3) exploring a new talent-training model to cultivate innovative and practical professionals in the cybersecurity field.
Keywords: cybersecurity; assurance system; threat; active defense; guard mode

一、前言

近年来，随着网络信息技术的不断发展，网络攻防对抗日趋频繁，网络安全领域面临一系列新的挑战。一是被保护目标更加多样。社交网络、政企内网、重大活动网络平台、关键信息基础设施等都是网络安全保障体系的保护目标[1]，不同的网络具有差异化的特点和网络安全防护等级需求。二是网络条件和场景环境不断变化。当前网络条件朝着更高速、更广泛、更智能的方向发展，云计算平台更是呈现出不确定的环境状态，网络场景环境呈现规模化、协同化、动态化的发展态势[2]。三是攻击源头和攻击手段更加隐蔽，未知攻击层出不穷[3]。随着攻防技术的持续演化，黑客的攻击手段也不断进化，未知攻击越来越多。高级可持续威胁攻击（APT）因其具有攻击持续性、技术专业性、目标针对性等特点，成为黑客组织广泛使用的网络攻击手段。四是系统保护目标可能不能完全配合保护者提出的相关保护要求。以国际运动赛事为例，比赛用信息系统所有者与保护者通常不属于一个国家，为保密起见，很难按照保护者的要求对其信息系统进行安全整改与加固，甚至可能不会去分享相应的安全信息，这为国际活动的安全保障带来了较大挑战。

目前，我国网络安全保障体系侧重于以“自卫模式”为核心的安全防护理念，依靠强健系统自身的防护能力来解决安全问题，如等级保护[4]、漏洞扫描[5]、护网演练、合规性测评[6]等。然而，这种被动式防御体系存在较多不足之处：一是主动探查能力不足，即防御者处于被动位置，只能在攻击行为发生之后采取措施；二是综合研判能力缺失，即不同开发商的信息系统和网络安全管理平台之间没有建立协同感知威胁情报研判中心，缺乏威胁情报数据的共享，不利于跨平台、跨域进行关联分析；三是协同处置能力偏弱，即隶属于不同机构的网络通常具有不同的安全等级，致使当前我国网络环境没有形成统一、跨设备、覆盖从应用层到网络层的协同处置体系。

以“自卫模式”为核心的网络安全保障体系在实际应用中稍显被动，可通过改变已有的被动防御为主动防御。例如，在 2022 年北京冬奥会和 2023 年第 31 届世界大学生夏季运动会的保障过程中，我国网络安全保障体系需要保护来自不同国家的信息系统，而这些系统的安全防护能力水平不一且无法对其提出额外的安全能力建设要求，使得仅依靠系统自身防护能力的“自卫模式”难以充分发挥作用。因此，在传统“自卫模式”的基础上，探索出一种以“护卫模式”为核心的新型主动安全防御体系，建立了一套集设陷探查、关联研判和应对拦截为一体的联动机制，实现了网络安全“零事故”的记录，提升了我国网络的安全性和可用性。

本文总结当前以“自卫模式”为主的网络安全保障体系发展现状，分析其面临的风险和挑战，在对比“护卫模式”“自卫模式”两种网络安全保障体系建设成本和保障层次的基础上，研判构建基于“护卫模式”的网络安全保障体系的重点任务，提出保障网络安全体系发展的对策建议，为新时期网络安全建设研究提供参考。

二、基于“自卫模式”的网络安全保障体系运行现状

（一）网络安全保障体系

国际上，为应对网络安全领域的挑战，美国等发达国家提出了基于动态保护的主动防御网络安全保障体系。美国在 2011 年提出“移动目标防御”的概念，通过部署随机动态变化的网络和系统来主动欺骗攻击者、扰乱攻击者视线、诱骗攻击者实施攻击行为，从而使攻击者触发告警，形成网络防御的主动态势。此外，美国国土安全部主导的网络空间安全自动监测项目“爱因斯坦”计划，通过对政府网络的入侵行为进行监测，保护政府网络的安全[7]；经过多年的迭代更新，实现了从被动防御到主动检测、从单一威胁分析到综合

威胁分析、从情报分析到情报共享、从单方负责到多方协同配合的演进。该计划在第一阶段采用网络流量检测引擎和网络流量分析技术，查找网络中的可疑行为；在第二阶段，采用入侵检测系统、恶意代码分析技术、安全信息与事件管理系统等构建网络空间信息共享与协作平台；在第三阶段，采用主动入侵防御系统自动检测网络威胁，实现主动网络安全防御。

近年来，美国积极开展对零信任架构的研究和应用。零信任架构假设网络中所有实体和网络流量均不可信，对网络中所有的访问请求都进行细粒度的身份认证；按照最小权限策略严格实施访问控制，以确保访问的安全性，同时访问控制策略随状态变化而动态调整[8]。理想的零信任网络架构核心逻辑组件通常包括策略执行点、策略引擎和策略管理员。当访问主体向策略执行点发送访问请求时，策略执行点将请求转发至策略引擎，策略引擎根据本地和外部的安全策略数据源对本次请求进行评估；策略管理员根据策略引擎的评估结果建立或者拒绝访问主体与资源之间的会话；当会话建立后，访问主体通过策略执行点与资源进行通信，在此过程中策略引擎持续进行信任评估，并将访问策略通过策略管理员转发给策略执行点进行更新；当发现存在风险时，策略执行点可以及时断开连接，起到快速保护资源安全的作用[9]。

在国内，网络空间拟态防御不再追求建立无漏洞、无后门、无缺陷的运行场景和防御环境，而是通过在软硬件系统中采取可迭代收敛的广义动态控制策略来防御网络空间的各种安全威胁[10~12]。该策略对当前运行的执行体集合进行不定期的变换，重构异构冗余体，通过虚拟化等技术改变运行环境配置，使系统对外呈现结构上的随机性和不可预测性[13]，从而使攻击者难以再次复现成功的攻击场景。

主动免疫可信计算是一种加强网络信息系统自身防护能力的网络安全保障体系。主动免疫可信计算技术采用运算和防护并行的新计算模式，以密码为基因进行身份识别、状态度量、保密存储，在统一管理策略支撑下对数据信息和系统服务资源进行可信检验判定，及时识别“自己”和“非己”成分，从而破坏和排斥进入机体的有害物质，为网络信息系统培育免疫免疫免疫能力，进而实现智能感知的主动防御。主动免疫可信计算技术适用于服务器、终端和嵌入式系统，可在行为源头判断异常并进行防范，实现已知病毒不查杀而自灭、未知病毒免疫抵御及利用未知漏洞的攻击；在结构上，可采取在处理器内部构建可信核模块、外接可信插卡、在主板内增加可信系统级芯片等方式安装防护部件，保障网络信息系统的安全。

（二）威胁探测

在网络威胁感知方面，当前以“自卫模式”为主的网络安全保障体系通常采用基于蜜罐技术的欺骗防御策略。HoneyToken[14]是基于蜜罐技术的典型欺骗防御策略，其本质是对攻击者感兴趣的目标进行去价值化伪造，如访问链接、文档、可执行文件、数据库入口等。Honeyfile[15]在Doc、PDF等格式的文档中嵌入可追踪和自动回溯的脚本代码，当攻击者打开文档时即可发送报警信息给Honeyfile的所有者。HoneyDatabase[16]通过故意设置存在漏洞且包含大量伪造机密信息的数据库来吸引攻击者访问。HoneyCredential[17]通过故意泄漏系统登录凭据来诱惑攻击者使用该凭据进行身份认证。HoneyAccount[18]通过故意泄漏类似管理员账号的方式来吸引攻击者登录，一旦该账号登录即判定为入侵行为并采取安全应急响应措施。

（三）攻击观测

以“自卫模式”为主的网络安全保障体系通常采用基于模式匹配的Web应用防火墙（WAF）等前置探测技术来为Web应用提供安全保障。基于模式匹配的WAF是一种典型的应用系统防护产品，其本质是通过检测访问服务器的数据流量来保护应用系统的安全。例如，通过基于签名的WAF来检测超文本传输协议（HTTP）请求中的异常流量，防止Web应用层遭受攻击[19]；或是采用多层缓存系统保证白名单的动态适用性，提高WAF的检测能力[20]。基于自学习的WAF，将Web应用的页面参数分为固定参数、列举参数和用户输入参数，对页面参数进行学习形成初始规则库，再通过持续学习扩大用户的正常行为模式，以适应用户的需求变化[21]；此外，还可以通过采用主动安全加固算法，提高WAF产品对会话劫持、HTTP隐藏按钮篡改、Cookie篡改等攻击的防御能力[22]。

（四）安全联动

以“自卫模式”为主的网络安全保障体系通常采用基于联动的网络安全管理策略。基于联动策略的网络安全运营中心是当前网络安全联动管理策略的一种主流形式。例如，天融信科技集团的安全管理系统可以对整个网络中的设备进行集中统一管理，监控网络状态，收集、过滤、分析各种安全产品的事件信息，并根据安全风险调整安全策略，作出快速响应。启明星辰信息技术集团股份有限公司的泰合信息安全运营中心为网络安全运营管理人员提供统一的安全策略配置方案，解决口令、认证、访问控制等方面的安全风险问题。美国思科公司推出基于IETF策略管理框架的服务质量（QoS）策略管理产品[23]，通过集中的QoS监测，实现策略控制盒转换过程的自动化，保障企业网络的服务质量。美国3Com公司提出的Transcend系统软件增加了虚拟局域网策略服务功能，管理人员可以集中设置虚拟局域网策略，并强制各个网络交换机执行。

（五）追踪溯源

以“自卫模式”为主的网络安全保障体系通常采用基于攻击行为感知的探测技术。采集攻击行为并进行感知分析是对攻击者进行追踪溯源的主要方式。蜜标技术[24]是一种追踪溯源的探测技术，可以在数据或文件中嵌入特定的标识信息，如脚本、统一资源定位符等。攻击者一旦访问标识信息，其操作行为会被记录并传回至远程服务器，管理员接收服务器告警并利用标识信息获取攻击者的网络地址、浏览器指纹等信息，从而溯源定位攻击者身份。此外，受害者通过路由调试技术[25]向上游路由器发送带有签名的攻击数据包，递归地调查上游链路，直到发现攻击者。基于互联网控制消息协议（ICMP）的追踪技术[26]要求每个路由器生成包含溯源信息的ICMP数据包，内有下一跳和上一跳的IP地址、时间戳、MAC地址等参数，通过分析该数据包即可溯源攻击者。

三、基于“自卫模式”的网络安全保障体系存在的问题

（一）“捕不全”问题

在网络威胁感知方面，当前我国网络安全保障体系是一种被动防御体系，只能在攻击者作出行动后才能被动地采集数据并分析攻击行为，这种方式往往难以提前、准确地感知攻击者的意图。因此，当前以“自卫模式”为主的网络安全保障体系对攻击行为存在“捕不全”的问题。一是蜜罐技术的设计初衷就是不拒绝任何人对其访问，因此访问者身份是不确定的，只能通过攻击者的行为来进行判断。如果攻击者采取的是未知攻击，不贸然地获取相关信息，那么即使攻击者进入了蜜罐，蜜罐也无法识别其身份，从而解决不了针对未知APT类攻击的捕捉。二是攻击探测面窄，传统蜜罐技术仅能就针对蜜罐实施攻击的行为作出反应，而对没有踩中蜜罐的攻击行为视而不见，易出现系统漏防的情况。三是易被攻击者识别，如果攻击者辨别出用户的系统为蜜罐，就会避免与该系统进行交互，并在蜜罐没有发觉的情况下潜入用户所在组织。

（二）“拦不住”问题

在网络入口防御方面，当前我国网络安全保障体系的保护对象多为用于日常管理的网络信息系统。经过多年的技术积累，这些系统依赖的软硬件环境各不相同，部分系统存在大量难以补救的安全漏洞、安全能力难以升级、易被各种攻击手段攻破。以“自卫模式”为主的网络安全保障体系对网络攻击行为存在“拦不住”的问题。一是网关防御仅对外部威胁有效，对内部威胁无法发挥作用；二是不支持加密HTTPS请求的分析和处理，对于加密流量的攻击行为无法探测；三是现有系统对基于源IP地址访问者的访问频次关注不够，而在实际攻防对抗过程中，首次访问和多次访问是需要给予不同关注度的；四是依靠规则进行防御的本质是防御已知威胁，攻击者了解WAF的防御机理，所采取的未知攻击手段能够规避WAF网关的检测，从而可以轻易地穿越WAF网关进行攻击；五是HTTP协议和业务场景的复杂性导致难以形成统一的策略规范，且WAF抽离于业务代码逻辑以外，攻击者应用这些耦合上的瑕疵可以绕过WAF防护系统，从而拦不住攻击者的网络攻击行为。

（三）“看不清”问题

在安全联动方面，当前我国网络安全保障体系仅依靠单个节点和事件很难判定APT行为。再加

上，我国现有的信息系统具有不同的安全等级且相互隔离，没有建立协同感知的威胁情报研判中心。因此，以“自卫模式”为主的网络安全保障体系对网络攻击行为存在“看不清”的问题。一是联动体系缺乏统一标准，各研究机构及安全设备厂商都有各自的描述语言、实现模型、协议和应用程序接口（API）函数，导致不同的安全策略管理系统/安全产品之间缺乏兼容性和互操作接口；二是仍需突破有关安全策略制定、存储、验证、查询和执行等方面的关键技术，特别是缺少对安全策略进行统一描述和对实际攻防环境进行定制的策略；三是现有的设备联动方法不能给出系统全面的全网解决方案，存在安全日志只报告不聚合、仅展示统计结果、不具备协同探测能力等不足。

（四）“抓不住”问题

在追踪溯源方面，当前我国网络安全保障体系主要关注如何防止各类攻击行为和有效检测未知网络威胁，易忽略攻击事件发生后的复盘分析，如对攻击者进行用户画像和对攻击行为进行溯源取证。因此，以“自卫模式”为主的网络安全保障体系对网络攻击行为存在“抓不住”的问题。一是探测手段相对单一，缺乏多轮次交互的粘随效果，对抗能力不强，如攻击者可以使用伪造的IP地址、代理服务等对抗网络溯源探测技术。二是网络追踪溯源技术多部署在攻击路径的靠后位置，虽然可以在一定程度上保护系统安全，却不能减少系统所遭受的攻击次数，更不能对系统所面临的未知网络威胁进行有效防御。三是已有的防御手段主要防范攻击行为而非攻击者，致使攻击者的攻击成本和代价较低，缺乏有效手段来甄别攻击者身份，无法有效震慑攻击者。

研究新型网络安全防御体系，提供更为健全的网络安全保障服务，成为推进我国信息化发展的迫切需要，对进一步加强和提升我国网络的安全性、可用性具有重要意义。

四、基于“护卫模式”的网络安全保障体系构建

（一）保障体系构建模式

1.“自卫模式”与“护卫模式”的对比

从防御模式来看，“自卫模式”是一种被动防御方式，以被保护目标为核心，具有“视野”较为狭窄、仅关注针对自身的攻击行为、需要不断跟踪最新攻击技术、需要根据新发现的攻击手段来被动发展针对性防护技术等特点。“护卫模式”则是一种主动防御方式，以护卫者为核心，支持护卫者可以从全局出发综合分析被保护系统的所有信息，更容易从更高的层面通过碰撞、关联等手段发现攻击者痕迹；可以根据资产状况进行针对性攻击探测，通过诱捕的方式主动发现攻击者，并研判其威胁等级。从防御视角来看，以“自卫模式”为代表的网络安全保障体系侧重于从局部视角发现攻击，在对特定目标进行攻击时，由于每个安全系统都是相互独立的，信息获取存在一定的不对称性和不确定性，极易产生误报或者难以研判的情况；以“护卫模式”为代表的网络安全保障体系则侧重于从全局视角发现攻击，通过全局联动将所有信息汇聚起来，并进行有序化安排，从而发现更多的攻击。

2. 保障体系框架

针对当前以“自卫模式”为主的网络安全保障体系仅能对既有行为进行异常分析、主动探查能力不足等问题，本研究构建了“护卫模式”网络安全保障体系研究框架（见图1）。“护卫模式”网络安全保障体系采用以“护卫模式”为主的主动式防御理念，以“欺骗诱捕、设陷探测”为思想指导，围绕设陷探测、攻击探查、安全联动和威慑溯源4个方面，发展近身蜜点、前置蜜庭、网关蜜阵、外溢蜜洞的“四蜜”威胁感知体系，涵盖支持纵深威胁感知的蜜点技术、支持攻击观测和判别的蜜庭技术、支持协同联动的蜜阵技术和支持网络威慑与攻击绘制的蜜洞技术。该网络安全保障体系提升了对高隐蔽攻击行为的感知和威慑能力，将现有的网络安全保障体系的防御重心从关注保护对象自身安全转变为发现和阻断攻击者，可为统筹构建国家级整体防御体系提供研究参考，有助于从根本上解决现有体系存在的四大安全问题。

（二）重点发展的技术任务

1. 支持纵深威胁感知的蜜点技术

在设陷探测方面，针对以“自卫模式”为主的网络安全保障体系面临的“捕不全”问题，“护卫模式”安全保障体系策略从被动防御变为主动探查。因此，新型的网络安全保障体系面向攻击者进

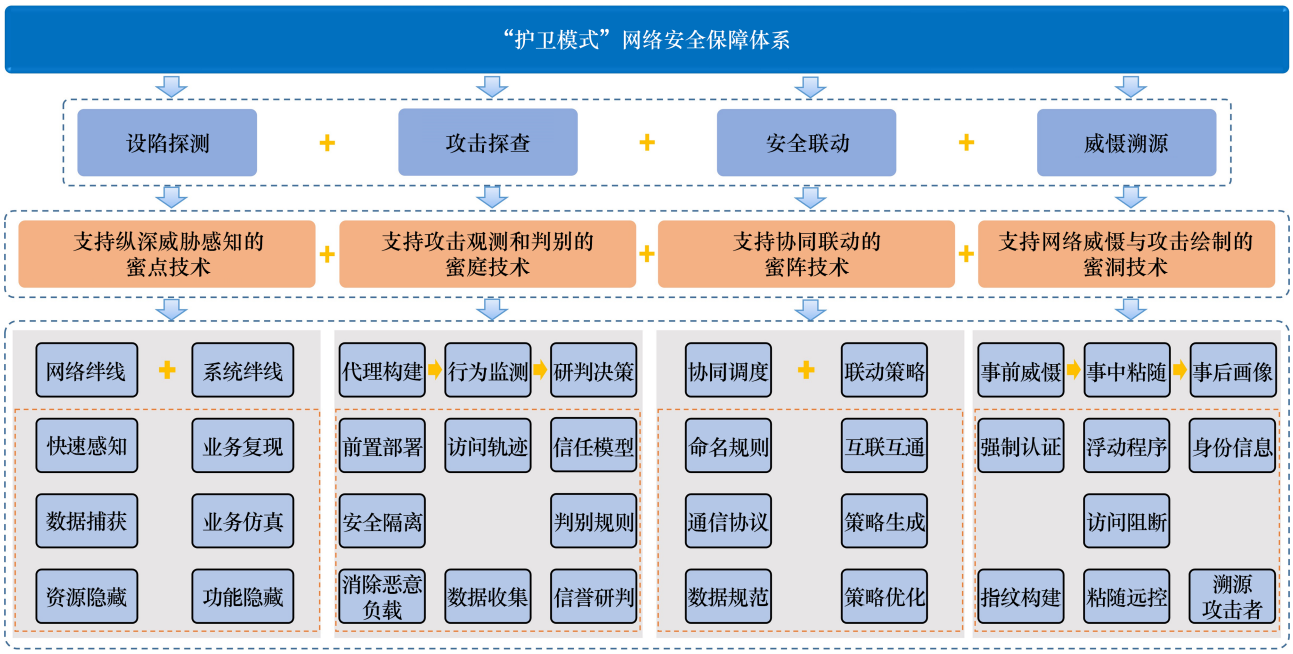

图1 “护卫模式”网络安全保障体系研究框架

入真实系统之前和之后两个阶段，通过在被保护系统周围部署大量多种蜜点等陷阱/绊线方式，全方位、多层次地主动感知系统面临的安全威胁。与蜜罐不同，蜜点并不主动散布自己的存在，而是放在常规用户不会访问的路径上，一旦蜜点被访问，则可确认该行为为非正常访问。在网络中，研究基于位置蜜点的网络绊线和系统绊线技术，即通过设置大量“自动触发器”，如地址围栏蜜点、域名变换蜜点、域控账号蜜点等，来防御系统外部面临的横向移动、域名爆破、域控制器等攻击，实现对网络攻击的主动防御。在系统内，研究基于寄生蜜点的系统绊线实现技术，即通过在系统服务中部署不会被正常用户使用的“暗功能”，或复现系统已有业务，部署功能诱饵蜜点、面包屑文件蜜点、特定账号密码蜜点和路径陷阱等寄生蜜点，隐藏真实功能和系统业务，防御攻击者对系统内部资源的获取，使攻击者即便突破了系统外围的防御，仍会在系统内部盗取资源时被发现，最终形成纵深安全威胁探测能力。

纵深威胁感知技术通过设置系统外部蜜点可快速感知外部威胁，一旦外部蜜点被触发，即可判断系统当前正在遭受攻击，使系统在网络攻击的起始阶段就有机会发现攻击者的动向。设置系统内部蜜点可更精准捕获攻击者行为，由于陷阱不会被用户的正常行为触发，因此内部蜜点一旦被触发即可以较高的置信度认定系统正在遭受入侵，从而定位入侵位置，实现对内部威胁的精准感知。总的来说，纵深威胁感知技术可以更全面地感知系统内外的安全态势，更早地发现针对系统的网络攻击，实现对攻击的快速响应。此外，在部署大量蜜点的系统中，攻击者需要花费更多的时间去甄别攻击目标，区分蜜点和真正的系统资源、系统漏洞，从而消耗攻击者的精力、增加攻击成本、降低攻击成功率。

2. 支持攻击观测和判别的蜜庭技术

在攻击探查方面，针对以“自卫模式”为主的网络安全保障体系所面临的“拦不住”问题，新型的网络安全保障体系通过部署可控的蜜庭等代理方式，既可以正常提供部分系统服务，让攻击者感觉不到并没有进入到真实的服务系统，又可以对攻击者进行访问轨迹研判，形成隐匿攻击判别能力。在攻击观测阶段，研究基于服务代理的前置蜜庭技术，即在蜜庭中构建外显相同的服务代理来建立与真实系统之间的安全隔离通道，以便消除恶意负载，提高代理响应速度，观察用户行为并进行数据收集。在攻击判别阶段，研究基于研判决策的信任判别方法，构建信任模型和用户 IP 信誉度判别规则，即对代理服务中的流量、命令、数据、网络连

接等行为数据进行监测和收集并上报研判中心。一旦攻击者试图通过不断变化来源IP地址来规避对其访问轨迹的观察时，研判中心就会对不断出现的新地址进行归并研判，从而发现潜在攻击者，实现对目标系统的前置防护。

攻击观测和判别技术将真实系统与外部网络环境进行安全隔离，降低了网络攻击直达系统所带来的安全风险。在攻击观测阶段，蜜庭可以观测攻击者的每一步行为，发现攻击者的攻击方式和攻击策略，为安全团队提供攻击数据的新视角，获取攻击者使用的工具和方法等信息。在攻击判别阶段，蜜庭可以对监测数据进行分析，全面判断用户行为所带来的影响，准确捕获由攻击行为所引起的系统数据异常，从而发现更隐蔽的网络攻击。此外，蜜庭收集到的监测数据也可以反映系统当前存在的安全漏洞和威胁，帮助安全人员提高系统的安全性，制定相应的安全策略。

3. 支持协同联动的蜜阵技术

在安全联动方面，针对以“自卫模式”为主的网络安全保障体系所面临的“看不清”问题，新型的网络安全保障体系对蜜点、蜜庭及传统防御设备进行统一调度，构建基于蜜阵的探测感知部署策略，形成全网联动的探测能力。首先，蜜阵整合蜜点、蜜庭等防御点，对其进行统一命名和管理，使防御点名字唯一且数据可区分。其次，蜜阵统一通信协议标准，定义数据规范和配置接口，实现蜜点、蜜庭、蜜阵的互联互通；同时，蜜阵为各防御点的管理、部署提供策略支持，根据系统安全态势实时调整防御点的类型和位置，建立主动防御措施的动态变化机制。最后，蜜阵根据专家知识库和历史攻击数据评价防御效果，分析防御点效用，迭代优化部署策略，降低防御成本，提高防御能力。

协同联动的蜜阵技术充分利用各安全系统和设备的优势，使其能够实时共享安全情报和攻击信息，增强系统应对安全威胁的能力；也有助于分析系统整体的网络安全状况并作出更加明智的决策，帮助整个安全系统迅速、全面地应对威胁，使网络安全保障体系更加全面高效。

4. 支持网络威慑与攻击绘制的蜜洞技术

在威慑溯源方面，针对以“自卫模式”为主的网络安全保障体系所面临的“抓不住”问题，新型的网络安全保障体系基于蜜洞对网络攻击者进行威慑并记录其身份信息，锁定攻击者，对攻击者进行画像绘制，形成“事前威慑、事中粘随、事后绘制”的跨越式攻击溯源能力。首先，蜜洞对所有访问用户的硬件设备编号、软件应用信息等唯一标识进行强制认证，构建指纹，跟踪用户行为。在攻击者获取关键资源时强制要求提供唯一标识，让攻击者意识到其行为已被发现，形成事前网络威慑，从而停止进一步攻击。其次，由于蜜洞向攻击者投递浮动程序，用以探查攻击者的资源和信息。对于原本要向攻击目标投递攻击程序的攻击者来说，需要接收对方投递过来的浮动程序，而攻击者通常会拒绝接受，从而暴露了其身份。因此，蜜洞技术可以实现对可疑行为的快速精准响应，并对非法访问进行阻断和粘随远控，使攻击者付出更高的成本和代价，达到持续性的粘随威慑效果。最后，蜜洞结合攻击者身份信息，绘制攻击者画像，将其镇定并溯源。

支持网络威慑与攻击绘制的蜜洞技术，可以有效震慑攻击者，增加攻击者的攻击成本和代价，降低系统被攻击的风险，减少系统受到的攻击次数和规模，保护系统和数据的安全。此外，还可以为攻击研判提供全面、详实的攻击者数据和情报，有效识别和溯源攻击者，辅助安全人员快速、有针对性地调整系统安全策略。

（三）重点发展的产业任务

在产业支撑方面，以“自卫模式”为主的网络安全保障体系侧重于被动抗打击和不被攻垮，难以有效支撑各领域的网络系统、适应日益突出的网络空间安全威胁和风险。以“护卫模式”为代表的网络安全保障体系侧重于预防攻击和发现攻击者，与网络安全保险产业相结合，有助于从整体上提高网络安全风险的治理水平，推动网络安全产业发展，为数字经济发展和网络强国建设提供重要支撑。

首先，在网络安全保险投保前的风险评估阶段，研判被保企业或单位的攻击感知能力，通过在被保企业设置蜜点的方式来提升企业对网络攻击的感知能力。其次，在网络安全保险的承保过程中，保险企业可以委托相应的安全支撑企业以低成本的方式在被保企业中广泛布设蜜点，并将其汇总到统

一的针对被保企业所构建的安全监测中心。该中心对所保护企业之间的攻击情况进行统筹，及时发现大范围的关联攻击，以最小的代价在最大的程度上及时发现攻击者的存在，降低网络安全事故的发生概率。一旦发现“踩蜜”行为，则意味着攻击者的身份暴露，被保企业可以立即进行整改并清理被访问的系统；安全支撑企业也可以通过日志溯源攻击者。最后，在出险后的响应和理赔阶段，如果造成损失的攻击者是已经被发现的“踩蜜者”，则需深入研究系统遭受攻击的原因，并依据保险合同中所明确的蜜点作用、蜜点处置规范和基于蜜点的免责条款等判断是否需要理赔及计算理赔额度。

发展由蜜点加持的网络安全保险产业，有助于被保企业构建并完善网络安全风险管理体系，强化网络安全风险应对能力，降低企业面临的网络安全压力，对构建新型的网络安全生态，促进数字经济的健康有序发展具有重要价值。

五、我国网络安全保障体系的发展建议

（一）探索“护卫模式”网络安全保障机制，全面提升国家网络安全防护水平

在现有基于“自卫模式”的网络安全保障体系的基础上，从国家层面制定相关政策法规引导和推动“护卫模式”网络安全保障体系的发展，将两种模式相结合，优势互补，全面提升国家网络安全防护水平。① 在政策引导方面，倡导构建以“四蜜”为代表的“护卫模式”网络安全保障体系，前期可通过意见、建议等形式对“护卫模式”安全防护技术及方案进行推广，后期可结合“网络安全等级保护 2.0 制度”等国家安全防护要求，将“护卫模式”相关要素融入国家标准。② 在资金支持方面，设立专项资金支持“护卫模式”网络安全保障体系的建设和应用推广，以科技攻关项目推动技术研发，突破核心关键技术，形成体系化技术方案，开展应用示范项目和试点工程以验证技术的有效性，并通过成功案例向企事业单位展示技术优势和应用前景。③ 在宣传教育方面，结合国家网络安全宣传周、重要网络安全学术会议等开展网络安全宣传、教育和学术活动，向研究人员、企业和公众介绍“护卫模式”网络安全保障体系的理念、技术、优势及应用效果，提高公众对“护卫模式”的认知，推动更多研究人员和企业的参与，促进“护卫模式”方案的推广和应用。

（二）探索“护卫模式”安全防护技术研究和应用，实现新旧安全防护技术的融合统一

建立“护卫模式”安全防护技术研发路线图，组织科研院所、网络安全企业等参与关键技术研究和平台开发，突破布陷感知、前置观测、协同联动以及粘随威慑等关键技术，构建“护卫模式”纵深威胁感知技术体系。同时，与现有的“自卫模式”安全防护技术（如可信防护、态势感知）结合，建立威胁共享和联动机制，实现新技术与原有技术的融合统一，有效支撑“护卫模式”技术的推广和应用。推动以“四蜜”为代表的“护卫模式”安全防护技术和应用的标准化，从架构体系、技术标准、部署标准、管理标准、网络安全等级保护要求等方面细化“护卫模式”技术及应用要求，增加新技术的可信度和推广力度，支撑开发者和用户进行技术开放共享与平台应用。推动“护卫模式”“杀手级”应用探索，面向工业、金融、通信等领域的关键信息基础设施，梳理“护卫模式”的应用需求；组织企业用户从实际应用和场景特点出发，提出符合企业需求的安全防护应用模式，以应用需求为导向对“护卫模式”相关技术和平台进行迭代更新，从而建立符合实际需求的技术体系和应用平台，并通过在关键信息基础设施上的应用，进一步验证“护卫模式”的有效性，形成良好的示范应用效果。

（三）探索面向“护卫模式”的网络安全人才培养新模式，培育创新实践型网络人才

面向“护卫模式”网络安全保障体系研发及应用需求，依托国家战略型人才和创新实践型人才培养目标，培养和挖掘一批具有战略视野、跨领域、创新思维、技能过硬的网络安全人才，形成人才培养战略规划。借鉴广州大学方滨兴院士班的“654321”网络安全人才培养模式，从人才培养具体实施角度，探索将“护卫模式”体系与网络安全人才培养相结合，将思辨能力和实践能力纳入人才培养目标，培育具有独立思考和技能过硬的创新实践型网络人才，推动“护卫模式”网络安全保障体系的不断进步。例如，“方班研讨厅”机制通过知名专家

和专业老师研讨点评的教学模式使学生快速掌握“求源、熵减、思辨”方法，从而培养创新和实践能力。探索人才培养与业务需求深度结合机制，将人才培养真正服务于安全防护需求，做好人才与需求对接，建立需求单位和人才之间的供需协调机制。例如，“方班演武堂”机制通过组织学生参与2022年北京冬季奥运会、2023年杭州第19届亚运会以及护网演练等大型活动网络安全保障任务，培养学生快速掌握“分析–验证–工程”方法，锻炼实战实践能力。积极鼓励民间团体组织各类网络攻防安全大赛，培养和挖掘“护卫模式”安全防护技术及运维人员，通过积极推进网络安全对抗，提升“护卫模式”的安全防护能力。

六、结语

本文针对当前“自卫模式”安全保障体系在应对APT攻击时所面临的“捕不全”“拦不住”“看不清”和“抓不住”等问题，提出了以“四蜜”为代表的“护卫模式”网络安全保障体系。“四蜜”威胁感知体系遵循“欺骗诱捕、设陷探测”的指导思想，使护卫者可以在暗处观察攻击者行为，发现其未知攻击的真相，从而更有效地锁定APT攻击者，显著降低发现APT攻击的时间。多次重大活动的网络安全保障案例均表明“四蜜”威胁感知体系在主动发现安全威胁、提高系统安全性方面发挥了重要作用。建议从政策引导、资金支撑、宣传教育、技术研发、标准规划、应用探索以及人才培养等多方面发展以“四蜜”为代表的“护卫模式”网络安全保障体系，提升对高隐蔽安全威胁的感知和威慑能力，以期能够开启统筹构建国家级整体防御体系的新阶段。

利益冲突声明

本文作者在此声明彼此之间不存在任何利益冲突或财务冲突。

Received date: August 22, 2023; **Revised date:** October 30, 2023

Corresponding author: Fang Binxing is a professor of the Cyberspace Institute of Advanced Technology, Guangzhou University, and a member of the Chinese Academy of Engineering. His major research field is cyberspace security. E-mail: fangbx@cae.cn

Funding project: Chinese Academy of Engineering project “Strategic Research of Cybersecurity Assurance System” (2022-JB-04)

参考文献

[1] 贾焰, 方滨兴, 李爱平, 等. 基于人工智能的网络空间安全防御战略研究 [J]. 中国工程科学, 2021, 23(3): 98–105.
Jia Y, Fang B X, Li A P, et al. Artificial intelligence enabled cyberspace security defense [J]. Strategic Study of CAE, 2021, 23(3): 98–105.

[2] Wu J X. Cyberspace endogenous safety and security [J]. Engineering, 2022, 15: 179–185.

[3] 方滨兴, 时金桥, 王忠儒, 等. 人工智能赋能网络攻击的安全威胁及应对策略 [J]. 中国工程科学, 2021, 23(3): 60–66.
Fang B X, Shi J Q, Wang Z R, et al. AI-enabled cyberspace attacks: Security risks and countermeasures [J]. Strategic Study of CAE, 2021, 23(3): 60–66.

[4] 王秋华, 吴国华, 魏东晓, 等. 工业互联网安全产业发展态势及路径研究 [J]. 中国工程科学, 2021, 23(2): 46–55.
Wang Q H, Wu G H, Wei D X, et al. Development trend and path of industrial Internet security industry in China [J]. Strategic Study of CAE, 2021, 23(2): 46–55.

[5] Jiang Z M, Tang Z F, Zhang P, et al. Programmable adaptive security scanning for networked microgrids [J]. Engineering, 2021, 7(8): 1087–1100.

[6] 马娟, 于广琛, 柯皓仁, 等. 工业互联网设备的网络安全管理与防护研究 [J]. 中国工程科学, 2021, 23(2): 81–87.
Ma J, Yu G C, Ke H R, et al. Network security management and protection of industrial Internet equipment [J]. Strategic Study of CAE, 2021, 23(2): 81–87.

[7] 安天研究院. 美国网络空间攻击与主动防御能力解析——美国网络空间安全主动防御体系 [J]. 网信军民融合, 2018 (2): 50–51.
ANTIY. Analysis of American cyberspace attacks and active defense capability—American cyberspace security active defense system [J]. Civil-Military Integration on Cyberspace, 2018 (2): 50–51.

[8] Bertino E. Zero trust architecture: Does it help? [J]. IEEE Security & Privacy, 2021, 19(5): 95–96.

[9] He Y H, Huang D C, Chen L, et al. A survey on zero trust architecture: Challenges and future trends [J]. Wireless Communications and Mobile Computing, 2022, 2022: 6476274.

[10] 斯雪明, 王伟, 曾俊杰, 等. 拟态防御基础理论研究综述 [J]. 中国工程科学, 2016, 18(6): 62–68.
Si X M, Wang W, Zeng J J, et al. A review of the basic theory of mimic defense [J]. Strategic Study of CAE, 2016, 18(6): 62–68.

[11] 罗兴国, 仝青, 张铮, 等. 拟态防御技术 [J]. 中国工程科学, 2016, 18(6): 69–73.
Luo X G, Tong Q, Zhang Z, et al. Mimic defense technology [J]. Strategic Study of CAE, 2016, 18(6): 69–73.

[12] Wang Y W, Wu J X, Guo Y F, et al. Scientific workflow execution system based on mimic defense in the cloud environment [J]. Frontiers of Information Technology & Electronic Engineering, 2018, 19(12): 1522–1536.

[13] Sepczuk M. Dynamic web application firewall detection supported by cyber mimic defense approach [J]. Journal of Network and Computer Applications, 2023, 213: 103596.

[14] Srinivasa S, Pedersen J M, Vasilomanolakis E. Towards systematic honeytoken fingerprinting [C]. Merkez: The 13th International Conference on Security of Information and Networks, 2020.

[15] Zhang L, Thing V L L. Three decades of deception techniques in active cyber defense: retrospect and outlook [J]. Computers & Security, 2021, 106: 102288.

[16] Osman A, Bruckner P, Salah H, et al. Sandnet: Towards high quality of deception in container-based microservice architectures [C]. Shanghai: IEEE International Conference on Communications, 2019.

[17] Qin X S, Jiang F, Cen M C, et al. Hybrid cyber defense strategies using honey-X: A survey [J]. Computer Networks, 2023, 230: 109776.

[18] Rauti S. A survey on countermeasures against man-in-the-browser attacks [C]. Bhopal: 19th International Conference on Hybrid Intelligent Systems, 2019.

[19] Amouei M, Rezvani M, Fateh M. RAT: Reinforcement-learning-driven and adaptive testing for vulnerability discovery in web application firewalls [J]. IEEE Transactions on Dependable and Secure Computing, 2022, 19(5): 3371–3386.

[20] Takahashi H, Ahmad H F, Mori K. Application for autonomous decentralized multi layers cache system to web application firewall [C]. Tokyo: The Tenth International Symposium on Autonomous Decentralized Systems, 2011.

[21] 李雪, 唐文, 张华. 一种新的Web应用防火墙的自学习模型 [J]. 小型微型计算机系统, 2014, 35(3): 483–487.
Li X, Tang W, Zhang H. New model of learning Web application firewall [J]. Journal of Chinese Computer Systems, 2014, 35(3): 483–487.

[22] 李莉, 翟征德. 一种基于Web应用防火墙的主动安全加固方案 [J]. 计算机工程与应用, 2011, 47(25): 104–106.
Li L, Zhai Z D. Web security enhancement scheme based on Web application firewall [J]. Computer Engineering and Applications, 2011, 47(25): 104–106.

[23] Bayazeed A, Khorzom K, Aljnidi M. A survey of self-coordination in self-organizing network [J]. Computer Networks, 2021, 196: 108222.

[24] 王瑶, 艾中良, 张先国. 基于蜜标和蜜罐的追踪溯源技术研究与实现 [J]. 信息技术, 2018 (3): 108–112.
Wang Y, Ai Z L, Zhang X G. Research and implementation of the network traceback technology based on honey-beacon and honeypot [J]. Information Technology, 2018 (3): 108–112.

[25] Zhao S Q, Lu Z, Wang C. Measurement integrity attacks against network tomography: Feasibility and defense [J]. IEEE Transactions on Dependable and Secure Computing, 2021, 18(6): 2617–2630.

[26] 姜建国, 王继志, 孔斌, 等. 网络攻击源追踪技术研究综述 [J]. 信息安全学报, 2018, 3(1): 111–131.
Jiang J G, Wang J Z, Kong B, et al. On the survey of network attack source traceback [J]. Journal of Cyber Security, 2018, 3(1): 111–131.