计算机科学
COMPUTER SCIENCE

网络安全主动防御技术:策略、方法和挑战

扈红超, 隋嘉祺, 张帅, 仝玉

引用本文

扈红超, 隋嘉祺, 张帅, 仝玉. 网络安全主动防御技术:策略、方法和挑战[J]. 计算机科学, 2024, 51(11A): 231100132-13.

HU Hongchao, SUI Jiaqi, ZHANG Shuai, TONG Yu. Proactive Defense Technology in Cyber Security:Strategies,Methods and Challenges [J]. Computer Science, 2024, 51(11A): 231100132-13.

计算机科学 COMPUTER SCIENCE
http://www.jsjkx.com
DOI:10.11896/jsjkx.231100132

网络安全主动防御技术:策略、方法和挑战

扈红超　隋嘉祺　张　帅　仝　玉
信息工程大学信息技术研究所　郑州 450001
(hhc@ndsc.com.cn)

摘　要　随着人工智能、云计算、大数据和物联网等新兴技术的迅速发展,网络安全形势变得日益严峻。然而,传统防御手段(如病毒查杀、漏洞扫描、入侵检测、身份认证、访问控制等)已无法有效抵御日益多样化的网络攻击,网络空间的防御与攻击之间出现了明显的不对称。为了扭转这种"易攻难守"的被动局面,学术界积极推动研发主动防御技术。其中,移动目标防御、欺骗防御和拟态防御3种技术发展迅速并日趋成熟。然而,目前很少有相关文献系统地归纳3种主流主动防御技术,也没有对3种技术进行横向对比和优劣分析。为了弥补这一空缺,对3种主动防御技术的研究成果进行了全面而系统的调查。首先,分别介绍了3种主动防御技术的概念、策略和方法,并根据研究内容的不同,对已有的研究成果进行分类。然后,对3种主动防御技术进行横向对比,分析它们之间的异同和优劣,并探讨如何将它们相互结合和补充,以增强主动防御技术的防护性能。最后,对3种主动防御技术面临的挑战和未来的发展趋势进行阐述。

关键词:主动防御;动态防御;移动目标防御;欺骗防御;拟态防御
中图分类号　TP393

Proactive Defense Technology in Cyber Security:Strategies,Methods and Challenges

HU Hongchao,SUI Jiaqi,ZHANG Shuai and TONG Yu
Institute of Information Technology,University of Information Engineering,Zhengzhou 450001,China

Abstract　Emerging technologies like artificial intelligence(AI),cloud computing,big data,and the Internet of Things(IoT) are developing quickly,making cybersecurity a vital issue. There is a clear asymmetry between cyberspace defense and attack,as the more sophisticated cyberattacks are beyond the reach of conventional defense strategies like intrusion detection,vulnerability scanning,virus detection,authentication,access control,etc. To counteract this state of passive vulnerability—which is "easy to attack but hard to defend"—academics have been actively pushing the study and creation of proactive defense technologies. Three such technologies—moving target defense,deception defense,and mimic defense—are maturing and developing quickly. Unfortunately,there is currently a dearth of literature that systematically summarizes the three proactive defensive mainstream technologies;additionally,there is no analysis of the advantages and disadvantages of the three technologies,nor a horizontal comparison. This work fills this vacuum by conducting a thorough and methodical evaluation of the research findings about the three proactive defensive strategies. Initially,the concepts,techniques,and methods of the three proactive defensive technologies are presented in their respective orders,and the current research findings are classified based on the various study topics. Subsequently,a horizontal comparison of the three proactive defense systems is conducted to examine their shared and unique characteristics,benefits and drawbacks,and potential synergies and complementarities that could improve the overall protection efficacy of these technologies. Lastly,the three proactive defensive technologies' difficulties and potential directions are discussed.

Keywords　Proactive defense,Dynamic defense,Moving target defense,Deception defense,Mimic defense

1　引言

随着人工智能、云计算、大数据和物联网等新兴技术的不断发展,信息资源在人们的日常生活和电力、交通、能源、航天等国家战略领域发挥着越来越重要的作用,深刻影响着当前的生产和生活方式。然而,随着互联网的普及,安全威胁不断增加,各种安全事件频繁发生,网络安全面临着严峻的挑战。尽管各个国家和组织都在积极采取措施来应对网络安全事件,但传统防御手段(如病毒查杀、漏洞扫描、入侵检测、身份认证、访问控制等)在面对日益多样化的攻击时只能提供有限的防护。这些传统方法无法解决攻击面广泛、未知攻击繁多以及人为因素复杂等问题,这导致防御者常常陷入被动、劣势的局面,无法有效应对当前存在的网络安全问题[1]。

为了扭转网络空间"易攻难守"的被动局面,创新防御机制,学术界积极推动研发主动防御技术。2011年12月,美国

基金项目:国家自然科学基金(62072467,62002383);国家重点研发计划(2021YFB1006200);河南省重大科技专项(221100211200)
This work was supported by the National Natural Science Foundation of China(62072467,62002383),National Key Research and Development Program of China(2021YFB1006200) and Major Science and Technology Project of Henan Province in China(221100211200).
通信作者:隋嘉祺(bearsui5@163.com)

国家科学技术委员会 NITRD 提出了“改变游戏规则”的革命性技术：移动目标防御(Moving Target Defence，MTD)；2013 年，国内的邬江兴院士提出拟态防御的思想；同时，以静态蜜罐演化而来的欺骗防御技术也在朝着动态、主动的方向发展。目前，以移动目标防御、欺骗防御、拟态防御为代表的主动防御技术发展迅速并日趋成熟，在产出大量科研成果的同时，广泛应用于云环境、区块链、智能电网等科学、工业领域。

现有的主动防御相关综述主要介绍了一种技术的策略或方法，同时也对 3 种技术进行了一定程度的比较：文献[2]中提出欺骗防御是移动目标防御的一部分；文献[3]在对欺骗防御分类时，将移动目标防御当成欺骗防御的一部分；文献[4]中则提出移动目标防御系统可以看作拟态防御系统的一个特例，它通过一些拟态变换使系统具有动态性特征，但是并没有应用异构冗余架构；文献[5]中也表达了相似的看法，即拟态防御思想是将移动目标防御的思想与异构冗余执行体相结合的产物。从上述研究中的观点可以看出，尽管 3 种主动防御技术之间没有明确定义的从属关系，但它们之间却有着紧密的联系。

现阶段，有关主动防御方面的综述性文章大多是针对单种技术的，如文献[2,6-11]是移动目标防御方面的综述，文献[3,12-21]是欺骗防御方面的综述，文献[4-5,22-27]是拟态防御方面的综述。很少有文章对 3 种主动防御技术进行系统的归纳总结，所以本文试图弥补这一空缺。首先，分别介绍了 3 种主动防御技术的的概念、策略和方法，并根据研究内容的不同，对已有的研究成果进行分类。然后，对 3 种主动防御技术进行横向对比，分析它们之间的异同和优劣，并探讨如何将它们相互结合和补充，以增强主动防御技术的防护性能。最后，对 3 种主动防御技术面临的挑战和未来的发展趋势进行阐述。

本文第 2 章介绍了移动目标防御技术的概念、策略和方法，并对其技术进行分类；第 3 章介绍了欺骗防御技术的概念、策略和方法，并对其技术进行分类；第 4 章介绍了拟态防御技术的概念、策略和方法，并对 DHR 架构进行详述；第 5 章对 3 种主动防御技术进行横向对比、结合互补；第 6 章分析了 3 种主动防御技术面临的挑战和未来发展趋势；最后总结全文工作。

2 移动目标防御

2.1 移动目标防御概述

2.1.1 移动目标防御的定义

移动目标防御(Moving Target Defence，MTD)是一种通过制定多样化、动态性的防御策略，持续性主动或被动地进行攻击面转换的主动防御机制。

1)攻击面(Attack Surface)指可以被攻击者利用来进行信息探测、资源窃取、系统破坏等攻击行为的系统资源的集合。时刻 t 的系统攻击面记为 $As(t)=\{p_1,p_2,\cdots,p_n\}$，其中 p_i 是 t 时刻某一攻击面的参数，如可以被攻击者利用的 IP 地址、端口号等系统资源。

2)攻击面转换指改变系统某一时刻的一个或多个攻击面参数，或改变某一攻击面参数在原攻击面的作用力大小。

部署移动目标防御的目的是使攻击者在一段时间内无法有效探测、收集信息或实施攻击行为，进而增加系统弹性，提高系统的主动防护水平[6-8]。

2.1.2 部署移动目标防御需要考虑的因素

1)确定需要保护的关键目标，并确定移动目标防御在网络中的部署位置，以提供更全面的保护；

2)需要在系统安全和性能之间进行平衡，同时考虑系统复杂性、资源需求和管理成本等因素[10]；

3)需要定期评估 MTD 策略的有效性，并及时更新防御机制和策略，以适应不断变化的威胁环境；

4)攻击者可能会采用高级手段来攻克 MTD 的防御策略，因此 MTD 应该与其他防御机制结合使用，形成多层次、综合性的安全防护体系。

2.2 移动目标防御的分类

现有的移动目标防御技术的研究，可以根据攻击面参数种类(what)、攻击面转换策略(how)、攻击面转换周期(when)和攻击面转换目的(prevention)等不同方式来进行分类。

由于不同分类方法存在一定的重叠，本文主要从 what 和 how 两种分类方式对移动目标防御技术进行阐述。

2.2.1 基于攻击面参数种类的分类

按移动目标防御中攻击面参数位于系统的不同层次，可将其分为网络层 MTD、数据层 MTD、系统层 MTD，如图 1 所示。

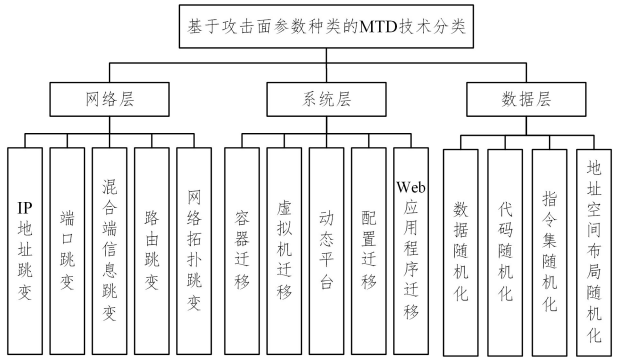


图 1 基于攻击面参数种类的 MTD 技术分类

Fig. 1 Classification of MTD techniques based on attack surface parameters

1)网络层

(1)IP 地址跳变指在传统网络或 SDN 网络中，通过周期性或随机性地跳变 IPv4 或 IPv6 地址来达到隐藏目标系统 IP 地址信息的目的。

Gudla 等通过 SDN 控制器给主机分配短暂的虚拟 IP 地址，采用离散的时间间隔进行虚拟 IP 跳变，同时建立真实 IP 地址和虚拟 IP 地址的映射，优化了 IP 地址跳变带来的网络不稳定和地址空间不足等问题[28]。Groat 等提出一个基于 IPv6 地址跳变的移动目标防御系统(MT6D)，由主机的 EUI-64 IID、共享会话密钥和时间戳 3 部分生成的哈希值，与主机子网拼接成动态跳变的 IPv6 地址，利用 IPv6 巨大的地址空间发挥地址跳变的优势[29]。

(2)端口跳变指周期性或随机性地跳变目标系统的服务端口来缓解针对服务的攻击。

Navas 等设计了一种 UDP 单端口跳变技术，通过输入的

静态参数 p 与伪随机二进制密钥流异或得到要跳变的端口号,有效地减轻了一些物联网环境下的网络攻击[30]。

(3)混合端信息跳变指同时进行 IP 地址和 MAC 地址、IP 地址和端口号等混合端信息的跳变,对网络嗅探、网络渗透等攻击起到很好的防护作用。

MacFarland 等通过 SDN 控制器对 DNS 查询进行修改,将虚拟 IP、MAC 地址与其真实地址的映射关系构成 NAT 转换表,客户端和服务器端使用虚拟 IP 和 MAC 地址建立连接,防止传输过程中的信息泄露[31]。Luo 等根据源标识(srcID)、服务标识(svcID)和时间进行不同模式下端口和地址的跳变,并由跳转网关执行真实到虚拟地址的转换,有效地抵御了扫描攻击和蠕虫病毒等网络攻击[32]。

(4)路由跳变指通过更改路由表项或控制 SDN 流表等方式,改变链路路由或路径参数,有效地缓解了链路洪泛攻击等问题。

Aydeger 等通过 ICMP 监控模块探查网络中存在大量 traceroute 操作的潜在攻击链路,然后查找包含该链路源主机和目的主机的其他链路,进行随机路由跳变,有效地缓解了链路洪泛攻击,减少了拥塞链路的问题[33]。Zhang 根据多种路由跳变约束选取符合条件的备选路径,通过路径权重值随机选取当前跳变路径,同时提出流表预下发策略,保证在路径切换过程中通信不中断,减小了路由跳变带来的时间开销[34]。

(5)网络拓扑跳变指周期性主动或被动地更改网络拓扑,使攻击者收集到的拓扑信息失效,进而一定程度上抵御了网络嗅探等攻击。

Rawski 提出的拓扑跳变策略,可以从预先计算好的配置中根据网络状态的安全等级周期性地选择变化,也可以由捕获的网络异常事件触发拓扑跳变[35]。Bai 等结合真实主机 IP、操作系统类型等信息和添加的虚假主机构造虚假网络拓扑,从跳变池中选择虚假网络拓扑进行随机拓扑跳变,并按照拓扑差异值决定当前虚假拓扑的存活时间[36]。

2)系统层

(1)容器迁移指将应用程序的镜像或容器镜像从一个主机或容器集群移动到另一个主机或容器集群,动态地改变系统的结构和配置,进而增加攻击者攻击系统的难度。

Azab 等通过入侵检测系统检测存在的持续性攻击,将原始采用的检查点/还原机制切换为容器实时迁移机制,并使用基于 Prey-vs-Predator 的博弈模型指导容器迁移,有效地检测并防止了持续性攻击[37]。Huang 等在进行容器动态迁移时,选择与原始容器差异较大的容器进行跳变,在迁移后从远程共享存储中恢复原始容器中的应用程序状态,并进行网络连接重定位、配置新 IP 地址等操作[38]。

(2)虚拟机迁移指在虚拟机运行的状态下,周期性地或随机地将虚拟机从一个物理主机或虚拟机迁移到另一个物理主机或虚拟机。

Penner 等开发设计了执行迁移所有 VM、只迁移攻击者收益最高的 VM、在每个节点中保留所有 VM 副本进行停用和迁移 3 种虚拟机迁移方案[39]。Debroy 等在进行虚拟机迁移的同时,对迁移频率优化,并根据候选 VM 的容量、可用带宽、历史信誉情况来选择最佳迁移位置[40]。

(3)动态平台指动态改变操作系统或硬件平台,通过更改其结构和软硬件配置来提高系统安全性。

Zhang 等提出在多个平台上按策略进行关键服务的迁移,并根据系统回报确定是否执行服务迁移和最优服务的迁移时机,并在迁移后重置当前平台[41]。Sourour 等设计在攻击频率较低的网络中,通过可信动态逻辑异构系统(TALENT),在多个候选平台中进行周期性的随机迁移,而在攻击频率较高的网络中,在 IDS 检测到入侵或未经授权的访问后进行实时的平台迁移[42]。

(4)配置迁移指周期性地或主动地将系统配置从一个状态迁移到另一个状态,或与欺骗性配置相结合,以提高系统的安全性。

Kong 等提出周期性地为每个容器生成、部署并映射具有欺骗性的系统配置组合,有效地防止了容器云中的信息泄露问题[43]。Lucas 等受进化的启发,使用之前良好的配置作为输入,经过复制、重组、变异和评估等操作生成更优的新配置,周期性地进行系统配置迁移[44]。

(5)Web 应用程序迁移指通过迁移策略将 Web 应用程序中的元素属性进行动态更改或迁移,以提高 Web 应用程序的安全性。

Sengupta 等通过博弈系统生成不同的迁移策略,周期性地切换 Web 应用程序的编码语言和数据库[45]。Niakanlahiji 等提出在攻击者进行探测和执行恶意代码的时间间隔中,将某些元素属性随机化,或随机添加新属性、新变量,并使用安全检查函数检查代码和元素的真实性,有效地防止了大量代码注入攻击[46]。

3)数据层

(1)数据随机化指将重要的数据信息进行随机化处理,如加密、哈希等操作,使得攻击者无法获取或解密数据,以增加攻击者获取数据的难度。

Cadar 等使用静态分析法将指令操作数分为不同等价类,为各类分配不同的随机掩码,使用对应掩码进行内存数据读取[47]。Man 等使用域敏感指针分析技术将数据分为不同等价类,为各类分配密钥并进行加解密[48]。

(2)代码随机化指将程序中的代码进行随机化处理,包括函数、数据结构和调用关系等,使得攻击者无法预测程序的行为。

Crane 等使用了新的基于编译器的代码转换和基于硬件的执行机制实现防御策略,有效抵御直接和间接的内存泄露及静态和动态的 ROP 攻击[49]。Pappas 等基于第三方应用程序一部分代码段的随机转化,可以直接应用在可执行文件上而不引入额外开销[50]。

(3)指令集随机化指对程序的指令集信息进行随机化处理,防止恶意代码的执行,有效地抵御了代码注入等攻击。

Gaurav 等通过生成对当前运行进程唯一的执行环境,创建特定于进程的随机指令集,使注入代码产生异常而无效化[51]。Fu 等通过多维哈希指令表、指令置换表和随机密钥对指令集进行转换,使指令集随机化来抵御代码注入攻击[52]。

(4)地址空间布局随机化指随机化内存中不同区域的地址空间布局,如堆、栈、进程地址、线程地址等,使攻击者无法准确定位攻击位置。

Seo 等提出了一种地址空间布局随机化的新方案 SGX-Shield，其可以引导内存空间布局实现更细粒度的随机化攻击频率较低的网络[53]。Fernando 等分析了内核随机化对共享内存的影响，在减轻内核攻击并提高安全性的同时，最大限度地节省了内存重复数据删除率[54]。

按攻击面参数种类(what)进行分类，可以更加细致地区分不同系统层次、不同防护组件的防御策略，有助于针对某一具体层次进行主动防护

2.2.2 基于攻击面转换策略的分类

根据攻击面转换策略的不同，MTD 大致可分为三大类：人工制定的随机策略，基于博弈论的攻击面转换策略，基于机器学习的攻击面转换策略，如图 2 所示。

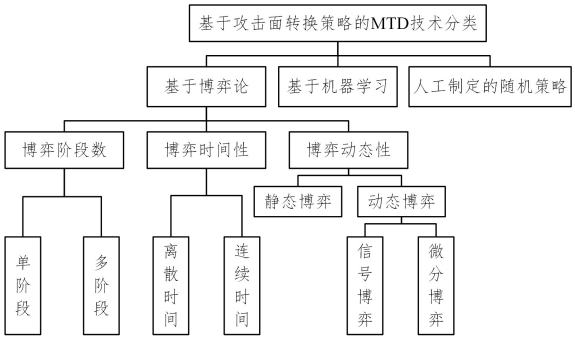


图 2 基于攻击面转换策略的 MTD 技术分类

Fig. 2 Classification of MTD Techniques based on attack surface transformation strategies

由于人工制定的随机策略没有固定的分类标准，且上文中提到的大多数策略都属于随机策略，因此本节不再重复讨论该类策略。本节主要介绍基于博弈论和基于机器学习的攻击面转换策略。

1)基于博弈论的攻击面转换

(1)根据博弈阶段数分类

①单阶段博弈指所有参与者在博弈开始时同时进行决策，并根据其他参与者的决策获得相应收益。

Jiang 仅考虑单阶段博弈系统，提出了一种基于信号博弈的移动目标防御决策模型，根据贝叶斯法则求解最优防御策略。但单阶段博弈模型只考虑了攻防过程中各种随机因素稳定不变的情况，并不符合真实网络攻防情景[55]。

②多阶段博弈指所有参与者可以在多个阶段进行决策，根据其他参与者的决策及时调整策略，每个阶段的决策都可能影响后续阶段的决策和收益。参与者之间进行相互博弈，力求自身收益最大化。多阶段博弈模型考虑了长期攻防对抗中，攻防策略改变等随机因素的影响，扩大了移动目标防御机制在攻防场景下的适用范围。

Chen 等根据攻防具有多阶段多状态的特性，提出一种移动目标 Markov 信号博弈模型，引入贝叶斯决策重新量化双方收益，加强高权重阶段中防御策略的制定[56]。

2)根据博弈时间性分类

①基于离散时间的博弈指在博弈过程中时间被离散化为一系列固定的时间点，所有参与者必须在指定的时间点进行决策。

Lei 等将 MTD 对抗过程看作离散时间序列上的多阶段动态事件，提出一种基于 Markov 博弈模型的移动目标防御系统，将攻防行为转化为攻击面和探测面的变化，提高了模型的通用性[57]。

②基于连续时间的博弈指在博弈过程中时间是连续的而不是离散的，所有参与者可以在任何的时间点进行决策。

Huang 等根据当前网络攻防过程中连续化、动态化的特点与传统博弈模型下时间离散、多阶段攻防的特性不同，提出一种网络攻防定性微分博弈模型，引入多维空间欧氏距离评估威胁程度，能够对安全威胁进行实时预警[58]。

3)根据博弈动态性分类

①静态博弈指所有参与者只能进行一次性决策，不能动态地多次选择。实际网络攻防对抗过程往往呈现动态性，采用静态博弈模型适用范围较小，要求攻击者和防御者同时做出选择，实用性不强。

Pratyusa 等提出一种基于静态博弈的防御模型，将攻防过程建模为双人博弈，利用博弈论来确定一种系统安全性和可用性之间较为均衡的最优防御策略[59]。

②动态博弈相较于静态博弈，更充分考虑了攻防双方行动的非同时性，双方采用实时行动进行攻防博弈，更加符合实际网络攻防场景。其中较为常见的是通过信号收发进行行动选择的信号博弈，以及参与者决策、收益都可由微分方程描述且连续可导的微分博弈。

Liu 等提出一种信号博弈模型，使用博弈模型和最优求解算法选取最优策略，并结合容器调度方法进行容器迁移，增强了云环境下的容器安全性[60]。Sun 等为了在时间连续、高频对抗的攻防过程中进行准确决策，提出一种微分博弈模型，利用微分博弈的开环纳什均衡求解算法得到最优防御策略，对网络关键节点进行实时防御[61]。

2)基于机器学习的攻击面转换

基于机器学习的防御策略是 MTD 的一种实现方式，它利用机器学习技术自动分析攻击行为，检测异常流量，激活跳变策略等，根据实时的网络状态动态调整网络防御策略，从而进一步提高系统的安全性和可靠性。

Gao 等提出了一种基于强化学习的自适应策略，与当前环境实时交互来自适应调整防御策略，同时通过算法参数来平衡系统的安全和性能问题，以满足不同的场景的需求[62]。Chai 等根据当前系统安全状态和攻防次数，使用深度学习算法动态调整、主动生成最优的跳变策略，进而找到网络安全性能与资源消耗之间的最优平衡点，在防御性能不降低的情况下，显著降低了网络资源消耗[63]。

按攻击面转换策略(how)进行分类，可以对移动目标防御的不同部署策略进行总结，有助于比较各种策略的优劣，进行策略之间的相互结合和补充，并确定不同策略适用的部署场景，进一步提高 MTD 的安全性能。

3 欺骗防御

3.1 欺骗防御概述

3.1.1 欺骗防御的定义

欺骗防御(Deception Defence)是一种通过掩饰目标特征信息或伪造蜜罐、蜜标等欺骗环境来收集攻击信息、重定向攻击流量、干扰攻击者认知、误导攻击决策的主动防御技术，可

以有效地阻碍网络攻击进程,增大攻击成本,从而增强目标系统的安全性能[12-15]。

3.1.2 部署欺骗防御需要考虑的因素

1)防御者部署的欺骗环境不能干扰真实业务系统的正常运行,并且需要在安全性和系统性能之间进行平衡。

2)防御者必须具有欺骗环境的控制权,能够辨别欺骗环境和真实业务系统的不同之处。在欺骗环境被攻击者识破并利用时,可以及时撤销欺骗环境,避免被当成跳板来执行更深层次的攻击。

3)防御者应根据具体业务环境的需求,调整欺骗资源的部署数量和部署范围[18]。

4)防御者应根据收集到的攻击信息和收益反馈,及时调整对不同攻击行为的防御策略部署。对多阶段、长时效的攻防过程采取灵活、动态、高效的欺骗防御方法[3]。

3.2 欺骗防御的分类

现有的欺骗防御技术的研究,可以根据欺骗资源的部署层次和欺骗防御的部署策略来进行分类,如图 3 所示。

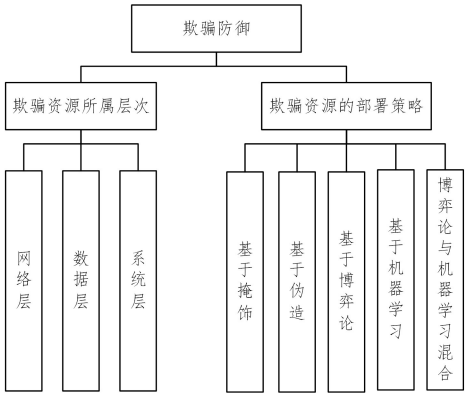


图 3 欺骗防御的分类

Fig. 3 Classification of deception defense

3.2.1 根据欺骗资源所属的系统层次进行分类

根据欺骗资源位于系统的不同层次,可以将欺骗防御技术分为网络层欺骗、数据层欺骗和系统层欺骗。

1)网络层

在蜜罐、蜜网等欺骗系统的网络层实施欺骗防御策略,如掩饰或伪造 IP 地址、端口号、拓扑等网络层特征信息,旨在诱骗攻击者捕获虚假的网络信息、重定向攻击,并主动捕获恶意网络流量,以达到欺骗攻击者的目的。

Zhang 等通过蜜网网关和入侵检测系统来检测、分析特定的恶意流量,利用 SDN 的流表特性,将指定类型的恶意流量无感知地重定向到对应类型的 Docker 蜜罐中[64]。Achleitner 等通过 SDN 控制器的流规则操纵网络流量,将其转发到欺骗服务器,当检测到探测行为时,欺骗服务器会为每一个主机创建虚拟网络拓扑,伪装关键资源,诱骗攻击者收集虚假信息[65]。

2)数据层

在数据层面部署虚假数据文件、虚假口令文件、诱饵文件和虚假补丁等欺骗实体,以达到告警攻击行为、消耗攻击资源、延缓攻击进程等欺骗目的。

Avery 等提出了一种由有效补丁和虚假补丁组成的 ghost 补丁,对攻击者分析、利用补丁漏洞产生误导效果,增加攻击耗费的资源和时间[66]。Juels 等设计在口令文件中增加多个虚假的用户名/密码哈希值,当虚假口令被攻击者利用时,会触发告警信息通知口令文件已被盗取[67]。

3)系统层

通过伪造或变换应用服务、程序、终端设备和指纹信息来构造欺骗环境,并制定相应的欺骗策略与攻击者进行交互,对攻击者进行更深层次的欺骗。

Zhou 等利用各类高仿真蜜罐、探针、诱饵等部件,针对网络攻击流程中的信息收集、入侵实现、提权维持、横向移动、痕迹消除等不同环节设置不同的欺骗防御手段,对网络攻击者进行深度欺骗[68]。Kyung 等设计了一种蜜网系统 HONEYPROXY,支持在低交互和高交互的蜜罐之间进行动态转换,将恶意攻击流量组播到相关的蜜罐中,并选择回送不包含指纹的响应,规避了指纹攻击[69]。Albanese 等提出的针对操作系统指纹识别和服务指纹识别的对抗方法,在不改变系统和服务配置的前提下,通过欺骗性流量和服务信息操纵来达到指纹混淆变换的效果[70]。

3.2.2 根据欺骗资源的部署策略进行分类

根据欺骗防御的部署策略,可以将欺骗防御分为基于掩饰的欺骗防御、基于伪造的欺骗防御、基于博弈论的欺骗防御、基于机器学习的欺骗防御和博弈论与机器学习混合的欺骗防御。

1)基于掩饰的欺骗防御指通过隐藏目标的特征信息,使攻击者无法获取真实的资源数据。部署策略类似于 MTD 的跳变机制,通过随机性和周期性地转换、更改或隐藏目标真实的资源特征,来干扰攻击者的认知,误导其攻击决策[18]。

Robertson 等为每个主机创建对应的网络视图,隐藏真实存在的资源,伪造不存在的虚假资源,将固定网络拓扑转换为具有欺骗性的、可调整的拓扑结构[71]。Lu 等制定双频率 IP 地址跳变策略,使用多个虚拟 IP 与主机真实 IP 相映射,并给真实主机和蜜罐主机配置不同的跳变频率,周期性地混淆网络拓扑信息[72]。

2)基于伪造的欺骗防御指通过使用蜜罐、蜜网、密标等虚假系统资源或伪造真实的系统资源,来构建欺骗环境,实现以下欺骗防御效果:告警攻击行为,收集攻击信息,进行虚假响应,重定向攻击流量,诱导攻击虚假资源。通过这些方法,可以达到延缓攻击进程、浪费攻击资源、增加攻击成本的欺骗目的。

Yang 等在 IDS 检测到的恶意攻击行为后,使用 OpenFlow 重新计算流量路由,将攻击者的请求重定向到指定蜜罐中,实现恶意流量的自动隔离[73]。Jia 等使用多个安装不同应用的蜜罐组成蜜罐簇,使整个蜜罐簇作为一个 Web 蜜罐对外发挥作用,在发现攻击时,根据攻击特征动态选择不同的应用蜜罐与攻击者进行交互[74]。

3)基于博弈论的欺骗防御指根据欺骗防御攻防过程多阶段、长时效的特点,结合博弈论思想来制定欺骗策略,包括诱捕机制的设计、诱捕点的分配等方面。使欺骗防御更符合真实环境中攻防双方互相博弈的流程,通过构建智能化的动态博弈诱捕场景,对攻击者实施更高级的欺骗手段。

Gao 等提出了一种基于多阶段随机博弈的虚拟化蜜罐动态部署机制 HoneyDep,在多阶段持续攻防的过程中追求防

御收益最大化，针对攻击者行为形成智能诱捕决策，进行高效策略部署，增强蜜罐部署的灵活性，提升防御诱捕效率[75]。Aliou 等考虑对抗过程中攻防双方的 zero-sum 博弈和攻击者可能采取的攻击集，计算纳什均衡下多样性蜜罐的最优多元化分配策略，得到蜜罐软件类型组合的最佳集，进而有助于最大化防御者收益[76]。

4)基于机器学习的欺骗防御。由于手动制定欺骗策略的成本较高，目前的研究重点是如何通过机器学习使计算机模拟人类行为，自动生成符合条件的欺骗策略和欺骗部件。同时，将强化学习与攻击诱捕相结合，以实现欺骗防御诱捕场景的自动化和智能化。

Abay 等通过深度学习算法和差分隐私技术来自动生成不同类型的欺骗性数据，并使用一个基于机器学习的度量标准来评估自动生成的欺骗数据的欺骗性，大大节省了部署欺骗数据的成本[77]。Kamel 等将防火墙判断的恶意数据流量重定向到蜜罐，通过机器学习算法对蜜罐中收集到的数据进行分析、概要、分类，并进一步预测新的攻击形式[78]。

5)博弈论与机器学习混合的欺骗防御。Song 提出单独使用博弈论或机器学习构造欺骗时存在一定的弊端[79]。单独使用博弈论时，存在蜜罐只能执行常规相应动作，没有综合考虑多轮攻防的全局最优策略，没有考虑攻击者使防御者信念变化对策略的影响，传统博弈难以处理大规模决策问题等弊端。而单独使用强化学习时，存在传统强化学习不适合进行大规模决策，对可动态调整的攻击策略可能不存在最优解等弊端。对此，提出将博弈论和深度强化学习结合使用，基于多轮次非合作不完全信息动态博弈模型，综合考虑博弈全过程中攻防信念对攻防策略的影响，提出了一种带有欺骗证据的蜜罐博弈机制(HoneyED)，允许蜜罐伪造输出来欺骗攻击者。同时，根据深度强化学习 Deep-CFR 算法设计实现了近似混合策略均衡求解算法，训练得到执行混合均衡策略的攻防智能体[79]。

将博弈论和机器学习相结合，可以互补二者单独使用时的不足，充分发挥它们的优势，优化欺骗防御制定策略并降低部署成本，进一步提高系统防御效能。

4 拟态防御

4.1 拟态防御概述

拟态防御(Mimic Defense)是一种借鉴生物学中的拟态现象，以动态异构冗余架构(Dynamic Heterogeneous Redundancy，DHR)为技术核心，在不改变目标对象功能的前提下，伪装服务功能外的其他行为，进而动态地改变其攻击面的主动防御技术[23-25]。

4.2 动态异构冗余架构

DHR 由输入代理、在线服务集、异构执行体集、异构组件池、调度器和表决输出器 6 部分组成，如图 4 所示。基于异构冗余原理，构建多套功能相同、结构不同的软硬件组合，并根据调度策略进行动态调度，能够增加系统的不确定性，从而提高攻击者对目标系统发起攻击的难度。

在一些已有的文献综述中，拟态防御系统中的拟态变换被按照网络层、平台层、数据层等部分进行分类[4,22]。但由于拟态防御与本文提到的其他两种主动防御技术有所不同，它的防御原理不仅仅涉及某一部分的变换，而是一个以动态异构冗余架构为核心，在全局行为上进行的变换策略。因此，本节从拟态防御的核心架构 DHR 出发，对 DHR 中的输入代理、在线服务集、异构执行体集、异构组件池、调度器和表决输出器 6 部分进行介绍，并详细阐述了不同部分的功能和策略，从 DHR 架构的角度对现阶段拟态防御的研究进行综述[24,26-27]。

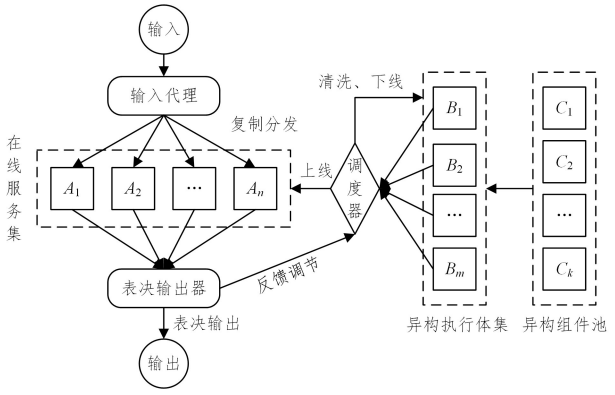


图 4 DHR 架构

Fig. 4 DHR architecture

1)输入代理

接受输入的消息并复制成 n 份，然后分发给异构执行体集中的 n 个异构执行体进行处理。在理论上，假设输入代理是安全的，不会受到攻击。

2)在线服务集

根据调度器的调度策略，从异构执行体集中选择 n 个异构执行体(n 一般为奇数)组成在线服务集。这些异构执行体分别对输入代理发来的消息进行处理，然后将处理结果送至表决输出器进行输出裁决，从而生成系统输出。

3)异构执行体池

由 m 个功能等价的异构执行体组成，当 m 的值越大时，理论上攻击者就越难攻破目标；并且，执行体之间的差异性越大，攻击者就越难利用执行体中的安全漏洞，拟态防御水平也就越高。

4)异构组件池

异构组件池中包含了不同系统层次的异构组件，按其构成要素所在层次进行分类，如图 5 所示。

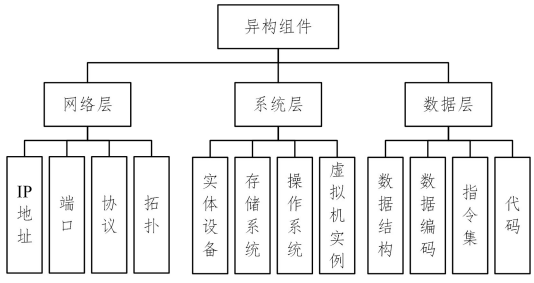


图 5 基于系统层次的异构组件分类

Fig. 5 Classification of heterogeneous components based on system hierarchy

根据制定的异构策略，将多个不同层次的异构组件相互组合和配置，形成了 k 个功能相同但结构不同的异构执行体，然后将它们部署进异构执行体池中，供拟态防御系统调度使

用。选择哪些异构组件来构建功能等价、结构不同且异构度较大的执行体，是拟态防御中一个关键环节。

5）调度器

调度器负责执行异构执行体的上线策略、下线策略和清洗策略，是 DHR 架构的核心部分。

（1）下线策略

将一个或多个服务集中的异构执行体下线，执行相关策略（隔离、清洗等）后放回异构执行体池中。现有的下线策略大致可分为定时下线、裁决下线、人工操作下线、混合策略下线等[26]。

①定时下线指定时选择服务集中的执行体进行下线处理。Li 等将在线执行体定时替换下线，在保持异构性的同时，减少每个异构执行体在服务集中出现的时间，降低持续性攻击的风险[80]。

②裁决下线指表决输出器对服务集中的多个执行体进行输出裁决，若存在异常情况，则对异常执行体进行下线处理。大部分拟态系统都采用此下线策略。

③人工操作下线指管理员主观决断后，手动对执行体进行下线操作，替换当前执行体。

④混合策略下线指多种下线方式相结合的下线策略。Song 等提出一种基于信任度的裁决下线和定时下线相结合的混合下线策略[81]。Pu 等设计通过 3 种方式触发下线调度策略，一是根据裁决器裁决结果；二是由管理者手工更换；三是根据时间片策略、随机冗余策略、监控策略等进行调度[82]。

（2）清洗策略

在处理替换下线的异构执行体时，常见的操作包括初始化、清零和状态回滚等简单的清洗策略。然而，这些策略并不能完全消除对执行体底层的攻击，如 Wei 等提出的基于执行体构件复位和状态恢复的清洗策略，在执行体被裁决为异常状态后，通过调度器会将异常执行体移出服务集，把执行体中各组件进行重启、复位，并通过之前保存的程序状态来进行执行体状态恢复[83]。此外，部分拟态系统也会对下线执行体进行构件重组等深度清洗策略[84]。

（3）上线策略

当执行策略将在线服务集中的异构执行体下线后，需要从异构执行体池中选择一定数量的执行体补充进入在线服务集。

①随机策略指随机选择异构执行体池中的执行体进入服务集中。Sang 提出一种完全随机调度算法，通过生成的伪随机数得到需要调度上线的执行体，对外完全呈现出一种不可预测的状态，且具有不可控性[85]。

②基于异构体属性参数的策略指根据异构执行体信任度、安全度、异构度、人工权重、防御能力等相关参数，制定相应的调度上线策略，从异构执行体的角度设计调度策略，最大化当前服务集的随机性，提高系统的异构性。如文献[86]中提出的调度器上线策略兼顾执行体的相异度和信誉度，选择相异度与信誉度都尽可能高的执行体集合，降低了共性缺陷出现的概率。Yu 等结合运行时长、运行开销、切换开销和执行体可信度等相关参数构造收益函数，为异构执行体调度提供依据[87]。Wang 等提出一种基于异构度和安全度的优先级调度算法，选择符合标准的异构执行体并结合时间片等动态策略进行执行体动态调度[88]。

6）表决输出器

通过制定的表决策略对 n 个异构执行体的输出结果进行表决后输出，随后调用调度器对执行体进行反馈调节。目前，可用的表决策略算法主要有全体一致表决算法、多数一致表决算法和多数一致性表决的改进算法。

多数一致表决算法中比较典型的是 k/n 表决算法。如果在 n 个异构执行体的输出结果中，有至少 k 个执行体的输出结果一致，那么将 k 个执行体的输出结果作为最终输出[89]。而多数一致性表决的改进算法是在多数一致表决算法的基础上，基于信誉度、异构度、错误率等相关参数进行的改进。在选择多数执行体输出结果时，考虑多个裁决因素，以降低协同攻击和共模攻击导致攻击逃逸的可能性。同时，提高输出结果的准确性和执行体的表决效率，以增强系统的拟态防御效能。

在现阶段的拟态防御系统中，大多使用多数一致表决算法的变体。如 Shen 设计的多模裁决器模块利用异构执行体信誉度，通过相关计算得到全局裁决结果，获得最接近真实情况的输出[86]。Wu 等将执行体各阶段的历史信息及攻击日志信息作为历史置信度参数，将执行体不同类别组件的异构性作为异构度参数，综合二者的平均度量值作为表决条件[90]。Gao 等综合考虑数据异常值和执行体表决赞同数两方面因素得到全局表决结果[91]。Yu 等根据执行体的动态可信度计算得到 n 个执行体输出结果的加权平均值，选择与平均值差异最小的执行体的输出结果作为最终的全局输出[87]。

5　3 种主动防御技术的对比与结合

移动目标防御（Moving Target Defence）、欺骗防御（Deception Defence）、拟态防御（Mimic Defence）同属于主动防御技术，旨在缓解传统防御手段无法满足当前网络攻防需求的问题。3 种技术采用积极主动的防御策略，力图改变当前网络“易攻难守”的不对称局面，提高网络弹性，增加攻击者实施攻击的难度和成本，从而提高防护目标的安全防御效能。

3 种主动防御技术关系紧密，存在很多相似之处，但防御思想和部署策略又不完全相同。三者有各自的优点和弊端，可以进行横向对比、结合互补，充分利用各自的优势来弥补自身不足，以最大程度地提高主动防御技术的防御性能。

5.1　横向对比

1）移动目标防御

移动目标防御是针对一种或几种特定属性进行变换的主动防御技术，具有更灵活的部署方式和更广泛的应用范围，旨在增加防御对象的弹性、动态性和复杂性。通过不断变化攻击面，减少攻击者利用系统脆弱性的机会，显著增加攻击者的攻击成本和攻击难度。对现有移动目标防御技术的分析总结如表 1 所列。

根据文献[92]的观点，大规模部署 MTD 可能会导致性能下降、服务延迟等问题，甚至会出现服务不可用的现象。因此，在设计移动目标防御策略时，需要在系统安全性、服务性能、资源利用率、部署成本等因素之间进行权衡，避免只注重安全性而影响系统的正常运行。同时，也要保证属性跳变时的可控性和有效性。

表 1 现有移动目标防御技术的分析总结

Table 1 Analytical summary of existing moving target defense techniques

分类标准		典型技术	防御策略	相关工作
基于攻击面的参数种类	网络层	IP 地址跳变	周期性或随机性地跳变目标系统的 IPv4 或 IPv6 地址	[28-29]
		端口跳变	周期性或随机性地跳变目标系统的服务端口	[30]
		混合端信息跳变	同时进行 IP 地址和 MAC 地址、IP 地址和端口号等混合端信息的跳变	[31-32]
		路由跳变	通过更改路由表项或控制 SDN 流表等方式，改变链路路由或路径参数	[33-34]
	系统层	网络拓扑跳变	周期性主动或被动地更改网络拓扑	[35-36]
		容器迁移	将应用程序的镜像或容器镜像进行迁移，动态地改变系统的结构和配置	[37-38]
		虚拟机迁移	周期性地或随机地将虚拟机从一个物理主机或虚拟机迁移到另一个物理主机或虚拟机	[39-40]
		动态平台	动态改变操作系统或硬件平台	[41-42]
		配置迁移	周期性地或主动地将系统配置从一个状态迁移到另一个状态	[43-44]
		Web 应用程序迁移	将 Web 应用程序中的元素属性进行动态更改或迁移	[45-46]
	数据层	数据随机化	将重要数据信息进行随机化处理，如加密、哈希等操作	[47-48]
		代码随机化	将程序中的代码进行随机化处理，包括函数、数据结构和调用关系等	[49-50]
		指令集随机化	对程序的指令集信息进行随机化处理，防止恶意代码的执行	[51-52]
		地址空间布局随机化	随机化内存中不同区域的地址空间布局，如堆、栈、进程地址、线程地址等	[53-54]
基于攻击面的转换策略		基于博弈论	攻防双方根据实际网络攻防场景进行攻防博弈，力求自身收益最大化，利用博弈论来确定一种系统安全性和可用性之间较为均衡的最优防御策略	[55-58,61]
		基于机器学习	利用机器学习技术自动分析攻击行为，检测异常流量，激活跳变策略等，根据实时的网络状态动态调整网络防御策略	[62-63]
		随机策略	由人工制定的随机策略	[28-54]

2)欺骗防御

在欺骗防御中，除了有类似移动目标防御的动态欺骗手段，还包含一些通过部署静态欺骗环境，对攻击者的攻击行为进行诱捕、欺骗的静态防御手段[16-17]。因此，欺骗防御比移动目标防御和拟态防御更具主动性。它不仅通过改变和伪装目标对象的特征来提高安全性，还会收集、分析恶意攻击行为，使用社会工程学手段，通过虚假信息来主动诱导攻击者改变其决策观念；同时，也使防御者更加了解攻击者的行为，有助于后续防御策略的修改和调整。对现有欺骗防御技术的分析总结如表 2 所列。

表 2 现有欺骗防御技术的分析总结

Table 2 Analytical summary of existing spoofing defence techniques

分类标准	防御策略	相关工作	
欺骗资源所属层次	网络层	在蜜罐、蜜网等欺骗系统的网络层实施欺骗防御策略，如掩饰或伪造 IP 地址、端口号、拓扑等网络层特征信息，诱骗攻击者捕获虚假的网络信息、重定向攻击，并主动捕获恶意网络流量	[64-65]
	系统层	通过伪造应用服务、应用程序和各种类型的终端设备来构造欺骗环境，并制定相应的欺骗策略与攻击者进行交互，对攻击者进行更深层次的欺骗	[68-70]
	数据层	在数据层面部署虚假数据文件、虚假口令文件、诱饵文件和虚假补丁等欺骗实体，以达到告警攻击行为、消耗攻击资源、延缓攻击进程等欺骗目的	[66-67]
欺骗资源的部署策略	基于掩饰	通过隐藏目标的特征信息，使攻击者无法获取真实的资源数据。部署策略类似于 MTD 的跳变机制，通过随机性和周期性地转换、更改或隐藏目标真实的资源特征，来干扰攻击者的认知，误导其攻击决策	[18,71-72]
	基于伪造	通过使用蜜罐、蜜网、密标等虚假系统资源或伪造真实的系统资源，来构建欺骗环境，达到告警攻击行为，收集攻击信息，进行虚假响应，重定向攻击流量，诱导攻击虚假资源等欺骗防御效果	[73-74]
	基于博弈论	根据欺骗防御攻防过程多阶段、长时效的特点，结合博弈论思想来制定欺骗策略，包括诱捕机制的设计、诱捕点的分配等方面，使欺骗防御更符合真实环境中攻防双方互相博弈的流程	[75-76]
	基于机器学习	通过机器学习模拟人类行为，自动生成符合条件的欺骗策略和欺骗部件。同时，将强化学习与攻击诱捕相结合，以实现欺骗防御诱捕场景的自动化和智能化	[77-78]
	博弈论与机器学习混合	将博弈论和机器学习结合使用，弥补二者单独使用时的不足，充分发挥各自的优势，优化欺骗防御制定策略并降低部署成本，进一步提高系统防御效能	[79]

相比于动态部署的主动防御策略，静态欺骗实体和资源的部署不需要频繁地变更系统，因此部署成本较低。然而，以蜜罐、蜜网为主的网络欺骗系统都存在动态性差、部署复杂、诱骗性不足以及维护困难等缺陷，这使得高级持续性威胁

(APT)攻击者仍然可以通过探测和分析绕过防御机制。此外,蜜罐一旦失效,不仅不能保护网络系统,还会被攻击者当作跳板去攻击其他资源[21]。因此,必须保证欺骗环境的可控性,并根据防御收益及时调整欺骗策略,在多阶段、长周期的攻防过程中,采取灵活、动态、高效的欺骗防御手段。

3)拟态防御

拟态防御的动态性依赖于拟态防御系统的动态冗余架构,它不局限于单个属性的变化,而是涉及整个系统架构的变革。

通过设计异构执行体,可以在一定程度上限制拟态系统的拟态变换范围。多个异构执行体进行的多模裁决显著提高了系统的安全性。对 DHR 架构中调度器的优化,则会进一步增强拟态系统的灵活性和稳定性。对调度器执行策略的分析总结如表 3 所列。

表 3　拟态防御中调度器执行策略的分析总结

Table 3　Analytical summary of scheduler execution strategies in mimic defense

分类	典型策略	防御策略	相关工作
下线策略	定时下线	定时选择服务集中的执行体进行下线处理	[80]
	裁决下线	表决输出器对服务集中的多个执行体进行输出裁决,若存在异常情况,则对异常执行体进行下线处理	[86-87,90]
	人工操作下线	管理员主观决断后,手动对执行体进行下线操作,替换当前执行体	[26]
	混合策略下线	多种下线方式相结合的下线策略	[81-82]
清洗策略	初始化、清零和状态回滚	通过不同方式对替换下线的异构执行体进行处理	[83-84]
上线策略	随机策略	随机选择异构执行体池中的执行体进入服务集	[85]
	基于异构体属性参数的策略	根据异构执行体信任度、安全度、异构度、人工权重、防御能力等相关参数,制定相应的调度上线策略,从异构执行体的角度设计调度策略,最大化当前服务集的随机性,提高系统的异构性	[86-88]

拟态防御系统不仅极大地增加了攻击者的攻击难度,还能实时检测出成功入侵的攻击行为,这是移动目标防御所不具备的[27]。但是,动态冗余架构在提升安全性的同时,也会引入巨大的部署开销。设计多个功能相同但结构不同的异构执行体需要全面考虑执行体的各个层次和不同组件,在设计、规划和执行时都需要投入大量的人力和物力资源。必要时,可以选择仅在核心层部署拟态防御策略,以提高系统安全性,并最大限度地节省部署成本。

本文前半部分对 3 种主动防御技术的防御策略进行了详细阐述和分类讨论。从讨论结果和上述比较可知,欺骗防御中的掩饰部分与移动目标防御的核心理念相似,旨在通过相关策略动态改变目标攻击面,掩饰系统真实的特征信息。而拟态防御则通过部署多个应用了类似 MTD 思想的异构执行体来提高系统的主动防御能力。由此可见,三者的核心防御理念相近,即通过动态性和多样性来增强安全性。而每种技术又有其独特的优势和不可避免的内生缺陷。理解这些技术的共通之处和差异性对于深入探究和有效运用主动防御策略至关重要,不仅有助于优化现有的防御策略,还为设计更高效、更全面的网络防御解决方案提供了基础。

5.2　结合互补

由于 3 种主动防御技术的防御思想和部署策略存在相似性,所以在设计防御手段时,可以将三者有效结合和相互补充。例如:

1)移动目标防御的跳变策略可以与欺骗防御的动态掩饰部分相互借鉴;

2)欺骗防御中欺骗资源的部署位置可以与移动目标防御中攻击面元素所在系统层次相互借鉴;

3)拟态防御的清洗、上线和下线策略可以与移动目标防御中的容器迁移、虚拟机迁移等系统层跳变策略相互借鉴;

4)移动目标防御不同系统层次的跳变策略可以应用到拟态防御异构执行体的设计中。

由于 3 种主动防御技术的侧重点不同,三者也可以在同一系统中同时部署,以弥补单一技术的内生缺陷,进一步增强系统的安全效能。例如:

1)将移动目标防御和欺骗防御结合使用。在制定 MTD 攻击面跳变策略时,部署与攻击面元素同类型的欺骗诱饵资源。这种方案显著提高了系统的混淆效果,弥补了单独部署欺骗环境时容易被攻击者识破绕过的缺陷,同时也加强了 MTD 的防御效能。文献[93]中通过生成的大量诱饵节点构造虚拟网络拓扑,并在此基础上结合 IP 随机化技术,即使攻击者识别出真实节点和诱饵节点,也会因为 IP 随机化使探测信息失效。

2)将拟态防御与欺骗防御结合使用。构建拟态防御系统的同时,部署诱饵节点进行欺骗防御。

3)将拟态防御与移动目标防御结合使用。当异构执行体进入在线服务集后,可以执行移动目标防御策略,改变自身攻击面元素,以增大在线异构执行体的弹性。

通过将 3 种主动防御技术有效结合和相互补充,可以充分发挥三者的优势,弥补各自的内生缺陷,实现更加综合的主动防御策略,对多类型安全威胁提供更为全面的保护,从多层次、多维度来提升防御效能,进而构建一个更加全面和强大的网络安全防御体系。

6　面临的挑战和未来发展趋势

目前,3 种主动防御技术正迅速发展并被广泛应用,对网络的安全性提升贡献显著。然而,这些技术在实施过程中也面临着一系列挑战。例如:主动防御的动态特性可能导致网络延迟增加和传输效率降低,对网络服务的整体质量产生负面影响。此外,主动防御的实施可能受到基础网络设施或软件组件固有缺陷的限制,这不仅限制了其防御效能,还可能引入新的安全隐患。再者,主动防御中频繁地变更策略可能会对系统的稳定性和可靠性造成影响,还可能与传统的网络安全防御技术相互干扰。重要的是,部署这些技术通常需要额外的计算资源、网络资源以及多个备用系统或组件,这不仅需要更多的技术支持和维护工作,也大幅提高了成本和运营开销。

因此,在实际部署主动防御策略时,要进行全面且准确的有效性、服务可用性、成本代价和防御效能评估,充分考虑服务质量、部署成本与安全性之间的平衡。根据实际网络环境中的评估结果,不断调整和优化主动防御策略,选择最合适当前应用场景的主动防御技术,尽可能发挥其防御效能。

传统的部署方式依赖防御人员的认知,需要手动分析恶意数据,制定攻防决策,并分配可用资源。然而,这种方式容易产生偏差和错误,且响应时间较长,降低了防护效率。

相较于人工制定的主动防御策略,基于人工智能和机器学习的防御策略展现出显著的优势。首先,这类策略制定方式可以通过分析大量的历史数据,如攻击行为、攻击模式以及攻防收益等信息,更精确地预测后续攻击,进而制定准确的防御策略。其次,它能持续学习和适应新数据及策略,随着时间的推进,提高决策的准确率,并极大地减少误判。此外,该方法具备实时响应的能力,能够快速且自主地调整策略,以实现更迅速和高效的部署。同时,它还有助于减少不必要资源的部署,从而在最大程度上降低运营成本。

因此,使用人工智能和机器学习技术来实现主动防御策略的自适应优化部署是未来一个重要的研究方向。

同时,主动防御技术在物联网、云环境和区块链等新型应用场景中也得到广泛的应用,但也面临着跨平台和多领域集成等重大挑战。需要充分考虑主动防御技术部署到各种新型应用场景时的特殊性,进一步适应各种规模和不同类型的部署环境,推动不同平台和领域之间的协同合作、相互融合。

未来的研究重点在于如何地将主动防御技术与其它新兴技术更好结合,以及如何将主动防御技术与其他新型应用场景良好兼容。这不仅需要进一步的技术创新和策略优化,还需深入理解各种应用场景的具体需求和挑战,进而促进主动防御技术术全面体系化发展,以显著提高各领域的安全性。

结束语 随着信息资源的迅猛发展,网络安全形势变得日益严峻。为了扭转传统防御手段导致的"易攻难守"的被动局面,学术界积极推动主动防御技术的研发,移动目标防御、欺骗防御、拟态防御应运而生。本文对3种主流的主动防御技术进行了系统的归纳总结。首先,分别介绍了3种主动防御技术的概念、策略和方法,并根据研究内容的不同,对已有的研究成果进行分类。然后,对3种主动防御技术进行横向对比,分析它们之间的异同和优劣,并探讨如何将它们相互结合和补充,以增强主动防御技术的防护性能。最后,对3种主动防御技术面临的挑战和未来的发展趋势进行阐述。本次研究系统地归纳、总结了3种主动防御技术在策略、方法方面的异同和缺陷,以及它们在技术层面面临的挑战和未来发展趋势,以期促进主动防御技术更好地发展。

参 考 文 献

[1] ZHENG Y, LI Z, XU X, et al. Dynamic defenses in cyber Security: Techniques, methods and challenges[J]. Digital Communications and Networks, 2022, 8: 422-435.

[2] CHO J H, SHARMA D P, ALAVIZADEH H, et al. Toward Proactive, Adaptive Defense: A Survey on Moving Target Defense[J]. IEEE Communications Surveys & Tutorials, 2020, 22(1): 709-745.

[3] FRAUNHOLZ D, ANTON S D, LIPPS C, et al. Demystifying deception technology: A survey[J]. arXiv: 1804.06196, 2018.

[4] SI M X, 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.

[5] YAO D, ZHANG Z, ZHANG G F, et al. A Survey on Multi-Variant Execution Security Defense Technology[J]. Journal of Cyber Security, 2020, 5(5): 77-94.

[6] ZHOU Y Y, CHENG G, GUO C S, et al. Survey onAttack Surface Dynamic Transfer Technology Based on Moving Target Defense[J]. Journal of Software, 2018, 29(9): 2799-2820.

[7] CAI G L, WANG B S, WANG T Z, et al. Research and Development of Moving Target Defense Technology[J]. Journal of Computer Research and Development, 2016, 53(5): 968-987.

[8] FAN L N, MA Y F, HUANG H, et al. The Research Summary of Moving Target Defense Technology[J]. Journal of CAEIT, 2017, 12(2): 209-214.

[9] JALOWSKIL, ZMUDA M, RAWSKI M. A Survey on Moving Target Defense for Networks: A Practical View[J]. Electronics, 2022, 11.

[10] SENGUPTA S, CHOWDHARY A, SABUR A, et al. A Survey of Moving Target Defenses for Network Security[J]. IEEE Communications Surveys & Tutorials, 2020, 22(3): 1909-1941.

[11] TAN J L, JIN H, ZHANG H Q, et al. A survey: When moving target defense meets game theory[J]. Computer Science Review, 2023, 48.

[12] LU Z, WANG C, ZHAO S Q. Cyber deception for computer and network security: Survey and challenges[J]. arXiv: 2007.14497, 2020.

[13] URIAS V E, STOUT W M S, LUC-WATSON J, et al. Technologies to enable cyber deception[C]// 2017 International Carnahan Conference on Security Technology (ICCST). IEEE, 2017: 1-6.

[14] LIEBOWITZ D, NEPAL S, MOORE K, et al. Deception for cyber defence: challenges and opportunities[C]// 2021 Third IEEE International Conference on Trust, Privacy and Security in Intelligent Systems and Applications (TPS-ISA). IEEE, 2021: 173-182.

[15] WANG C, LU Z. Cyber deception: Overview and the road ahead [J]. IEEE Security & Privacy, 2018, 16(2): 80-85.

[16] RAUTI S, LEPPÄNEN V. A survey on fake entities as a method to detect and monitor malicious activity[C]// 2017 25th Euromicro international conference on Parallel, Distributed and Network-based Processing (PDP). IEEE, 2017: 386-390.

[17] ZHANG L, THING V L L. Three decades of deception techniques in active cyber defense-retrospect and outlook[J]. Computers & Security, 2021, 106: 102288.

[18] JIA Z P, FANG B X, LIU C G, et al. Survey on cyber deception [J]. Journal on Communications, 2017, 38(12): 128-143.

[19] GAO Y Z, LIU Y Q, XING C Y, et al. Research on Network Deception Defense Oriented Attack Trapping Technology[J]. Computer Technology and Development, 2022, 32(3): 114-119.

[20] ZHU M, ANWAR A H, WAN Z, et al. Game-theoretic and machine learning-based approaches for defensive deception: A sur-

vey[J]. arXiv:2101.10121,2021.

[21] ZHU M,ANWAR A H,WAN Z,et al. A survey of defensive deception:Approaches using game theory and machine learning [J]. IEEE Communications Surveys & Tutorials,2021,23(4):2460-2493.

[22] LI G S,WANG W,GAI K,et al. A framework for mimic defense system in cyberspace[J]. Journal of Signal Processing Systems,2021,93:169-185.

[23] MA B,ZHANG Z. Security research of redundancy in mimic defense system[C]// 2017 3rd IEEE International Conference on Computer and Communications(ICCC). IEEE,2017:2910-2914.

[24] WU J X. Research on Cyber Mimic Defense[J]. Journal of Cyber Security,2016,1(4):1-10.

[25] WU J X. Meaning and Vision of Mimic Computing and Mimic Security Defense[J]. Telecommunications Science,2014,30(7):2-7.

[26] MA H L,YI P,JIANG Y M,et al. Dynamic Heterogeneous Redundancy based Router Architecture with Mimic Defenses[J]. Journal of Cyber Security,2017,2(1):29-42.

[27] HU H C,CHEN F C,WANG Z P. Performance Evaluations on DHR for Cyberspace Mimic Defense[J]. Journal of Cyber Security,2016,1(4):40-51.

[28] GUDLA C,SUNG A H. Moving Target Defense Discrete Host Address Mutation and Analysis in SDN[C]// International Conference on Computational Science and Computational Intelligence. 2020:16-18.

[29] DUNLOP M,GROAT S,URBANSKI W,et al. MT6D:A Moving Target IPv6 Defense[C]// MILCOM 2011 Military Communications Conference. 2011.

[30] NAVAS R E,SANDAKE H,FREDERIC C,et al. IANVS:A Moving Target Defense Framework for a Resilient Internet of Things[C]// 2020 IEEE Symposium on Computers and Communications(ISCC). 2020.

[31] MACFARLAND D,SHUE C. The SDN Shuffle:Creating a Moving-Target Defense using Host-based Software-Defined Networking[C]// ACM Workshop on Moving Target Defense. 2015:37-41.

[32] LUO Y B,WANG B S,WANG X F,et al. RPAH:Random Port and Address Hopping for Thwarting Internal and External Adversaries[C]// 2015 IEEE Trustcom/BigDataSE/ISPA. 2015:20-22.

[33] AYDEGER A,SAPUTRO N,AKKAYA K,et al. Mitigating Crossfire Attacks Using SDN-Based Moving Target Defense [C]// 2016 IEEE 41st Conference on Local Computer Networks (LCN). 2016.

[34] ZHANG B F. Research on Moving Target Defense Based on Network Layer in SDN [D]. Tianjin: Tianjin University of Technology,2022.

[35] RAWSKI M. Network Topology Mutation as Moving Target Defense for Corporate Networks[J]. INTL Journal of Electronics and Telecommunications,2019:571-577.

[36] BAI S H,ZHANG Z,LIU S X. Proactive Defense Method Based on False Network Topology Hopping[J]. Journal of Information Engineering University,2022,23(3):337-343.

[37] AZAB M,MOKHTAR B,ABED A,et al. Toward Smart Moving Target Defense for Linux Container Resiliency[C]// 2016 IEEE 41st Conference on Local Computer Networks(LCN). 2016.

[38] HUANG R,ZHANG H Q,LIU Y. RELOCATE:A Container Based Moving Target Defense Approach[C]// CENet 2017-the 7th International Conference on Computer Engineering and Networks. 2017.

[39] PENNER T,GUIRGUIS M. Combating the Bandits in the Cloud:A Moving Target Defense Approach[C]// ACM International Symposium on Cluster,Cloud and Grid Computing. 2017.

[40] DEBROY S,CALYAM P,NGUYEN M,et al. Frequency-minimal moving target defense using software-defined networking [C]// International Conference on Computing. 2016.

[41] ZHANG Y P,CHANG X L,MIŠIĆ J J,et al. Cost-effective migration-based dynamic platform defense technique:a CTMDP approach[J]. Networking and Applications, 2021, 14: 1207-1217.

[42] SOUROUR D,CHEN T R,FENG Y,et al. Platform Moving Target Defense Strategy Based on Trusted Dynamic Logical Heterogeneity System[C]// International Conference on Artificial Intelligence and Computer Science. 2019.

[43] KONG T,WANG L M,MA D H,et al. ConfigRand:A Moving Target Defense Framework against the Shared Kernel Information Leakages for Container-based Cloud [C] // International Conference on High Performance Computing and Communications;International Conference on Smart City. IEEE International Conference on Data Science and Systems,2020.

[44] LUCAS B,FULP E W,JOHN D J,et al. An Initial Framework for Evolving Computer Configurations as a Moving Target Defense[C] // Cyber and Information Security Research Conference. 2014.

[45] SENGUPTA S,VADLAMUDI S G,KAMBHAMPATI S,et al. A Game Theoretic Approach to Strategy Generation for Moving Target Defense in Web Applications[C]// 16th Conference on Autonomous Agents and MultiAgent Systems. 2017:178-186.

[46] NIAKANLAHIJI A,JAFARIAN J. WebMTD:Defeating Web Code Injection Attacks using Web Element Attribute Mutation [C]// 4th ACM Workshop on Moving Target Defense. 2017:17-26.

[47] CADAR C,AKRITIDIS P,COSTA M,et al. Data Randomization:Technical Report:TR-2008-120[R]. Microsoft Research, 2008.

[48] MAN Y J,YIN Q,ZHU X D. Fine-grained data randomization technique based on field-sensitive pointer analysis[J]. Journal of Computer Applications,2016,36(6):1567-1572.

[49] CRANE S,LIEBCHEN C,HOMESCU A,et al. Readactor:Practical Code Randomization Resilient to Memory Disclosure [C]// IEEE Symposium on Security and Privacy. 2015.

[50] PAPPAS V,POLYCHRONAKIS M,KEROMYTIS A D. Smashing the Gadgets:Hindering Return-Oriented Programming Using In-Place Code Randomization[C]// IEEE Symposium on Security and Privacy. 2012.

[51] KC G S,KEROMYTIS A D,PREVELAKIS V. Countering

Code-InjectionAttacks With Instruction-Set Randomization [C]// ACM Conference on Computer and Communications Security. 2003: 272-280.

[52] FU J M, ZHANG X, LIN Y. An Instruction-Set Randomization Using Length-Preserving Permutation [C]// IEEE Trustcom/BigDataSE/ISPA. 2015.

[53] SEO J, LEE B, KIM S M, et al. SGX-Shield: Enabling Address Space Layout Randomization for SGX Programs [C]// Network and Distributed System Security Symposium. 2017.

[54] VANO-GARCIA F, MARCO-GISBERT H. KASLR-MT: Kernel Address Space Layout Randomization for Multi-Tenant Cloud Systems [J]. Journal of Parallel and Distributed Computing, 2019, 137: 77-90.

[55] JIANG L. Research on Moving Target Defense Decision-making Method Based on Dynamic Attack-defense Game Model [D]. Zhengzhou: PLA Strategic Support Force Information Engineering University, 2019.

[56] CHEN Y, WANG G C. Research on Defense Decision Optimization of Moving Target Markov Signaling Game [J]. Journal of Chinese Computer Systems, 2023, 44(2): 392-400.

[57] LEI C, MA D H, ZHANG H Q. Optimal Strategy Selection for Moving Target Defense Based on Markov Game [J]. IEEE Access, 2017, 5: 156-169.

[58] HUANG S R, ZHANG H W, WANG J D, et al. Network security threat warning method based on qualitative differential game [J]. Journal on Communications, 2018, 39(8): 29-36.

[59] MANADHATAP K. Game Theoretic Approaches to Attack Surface Shifting [M]// Moving Target Defense II: Appication of Game Theory and Adversarial Modeling. New York: Springer, 2012: 1-13

[60] LIU D Q, HU H C, HUO S M. Container migration strategy based on moving target defense signaling game [J]. Application Research of Computers, 2023, 40(3): 890-897.

[61] SUN Y, JI W F, WENG J, et al. Optimal Strategy of Moving Target Defense Based on Differential Game [J]. Journal of Computer Research and Development, 2021, 58(8): 1789-1800.

[62] GAOC G, WANG Y J. Reinforcement learning based self-adaptive moving target defense against DDoS attacks [C]// International Conference on Electronics, Communications and Information Technology (CECIT). 2020: 26-28.

[63] CHAI X Z, WANG Y S, YAN C X, et al. DQ-MOTAG: Deep Reinforcement Learning-based Moving Target Defense Against DDoS Attacks [C]// 2020 IEEE Fifth International Conference on Data Science in Cyberspace (DSC), 2020.

[64] ZHANG W, XU Z G, CHEN Y F, et al. Design and Implementation of a SDN Honeynet Based on Dynamic Docker [J]. Netinfo Security, 2022, 22(4): 40-48.

[65] ACHLEITNER S, PORTA T F L, MCDANIEL P, et al. Deceiving Network Reconnaissance Using SDN-Based Virtual Topologies [J]. IEEE Transactions on Network and Service Management, 2017: 1098-1112.

[66] AVERY J, SPAFFORD E H. Ghost Patches: Fake Patches for Fake Vulnerabilities [C]// IFIP Advances in Information and Communication Technology. 2017.

[67] JUELS A, RIVEST R L. Honeywords: making password-cracking detectable [C]// ACM Sigsac Conference on Computer & Communications Security. 2022.

[68] ZHOU Y, WU Z, YANG Z T, et al. Research on Dynamic Adaptive Network Security Defense Based on Deception Defense [J]. Technology Research, 2022, 3: 54-60.

[69] KYUNG S, HAN W, TIWARI N, et al. HoneyProxy: Design and implementation of next-generation honeynet via SDN [C]// IEEE Conference on Communications and Network Security (CNS). 2017.

[70] ALBANESE M, BATTISTA E, JAJODIA S. A deception based approach for defeating OS and service fingerprinting [C]// 2015 IEEE Conference on Communications and Network Security (CNS). IEEE, 2015: 317-325.

[71] ROBERTSON S, ALEXANDER S, MICALLEF J, et al. CINDAM: Customized Information Networks for Deception and Attack Mitigation [C]// IEEE International Conference on Self-adaptive & Self-organizing Systems Workshops. 2015.

[72] LU X Y, YI P, BU Y J, et al. SDN Honeynet Based on Network Deception Mechanism [J]. Journal of Information Engineering University, 2022, 23(4): 471-477.

[73] YANG T S, DIAO P J, LIANG L L, et al. Active Forensics Technology of Honeypot Based on OpenFlow [J]. Transactions of Beijing Institute of Technology, 2019, 39(5): 545-550.

[74] JIA Z P, FANG B X, CUI X, et al. ArkHoney: A Web Honeypot Based on COllaborative Mechanisms [J]. Chinese Journal of Computers, 2018, 41(2): 413-425.

[75] GAO Y Z, LIU Y Q, ZHANG G M, et al. Multi-stage Game Based Dynamic Deployment Mechanism of Virtualized Honeypots [J]. Computer Science, 2021, 48(10): 294-300.

[76] SARR A B, ANWARA H, KAMHOUA C, et al. Software Diversity for Cyber Deception [C]// GLOBECOM 2020-2020 IEEE Global Communications Conference. 2020.

[77] ABAY N C, AKCORA C G, ZHOU Y, et al. Using Deep Learning to Generate Relational HoneyData [J]. Autonomous Cyber Deception, 2019: 3-19.

[78] EDDABBAH M, LMOUMEN Y, TOUAHNI R. A Smart Agent Design for Cyber Security Based on Honeypot and Machine Learning [J]. Hindawi, Security and Communication Networks, 2020, 2020(1): 8865474.

[79] SONG L H, JIANG Y Y, XING C Y, et al. Optimization mechanism of attack and defense strategy in honeypot game with evidence for deception [J]. Journal on Communications, 2022, 41(11): 104-116.

[80] LI C H, TANG J J, CHEN Y T, et al. Dynamic scheduling method of service function chain executors based on the mimic defense architecture [J]. Telecommunications Science, 2022, 38(4): 101-112.

[81] SONG K, LIU Q R, WEI S, et al. Endogenous security architecture of Ethernet switch based on mimic defense [J]. Journal on Communications, 2020, 41(5): 18-26.

[82] PU L M, WEI H Q, LI X, et al. Mimic cloud service architecture for cloud applications [J]. Chinese Journal of Network and Information Security, 2021, 7(1): 101-112.

[83] WEI S, YU H, GU Z Y, et al. Architecture of Mimic Security Processor for Industry Control System[J]. Journal of Cyber Security, 2017, 2(1): 54-73.

[84] MA H L, WANG L, HU T, et al. Survey on the development of mimic defense in cyberspace: from mimic concept to "mimic+" ecology[J]. Chinese Journal of Network and Information Security, 2022, 8(2): 15-38.

[85] SANG X N. Research on dynamic scheduling algorithm for mimic defense architecture[D]. Nanjing: Nanjing University of Science and Technology.

[86] SHEN C Q, CHEN S X, WU C M, et al. Adaptive mimic defensive controller framework based on reputation and dissimilarity [J]. Journal on Communications, 2018, 39(s2): 173-180.

[87] YU F, LIU K, GENG Y Y, et al. Multi executor decision algorithm and scheduling algorithm based on differential distance feedback[J]. Application Research of Computers, 2022, 39(5): 1437-1443.

[88] WANG R M, XING Y X, SONG W, et al. Secure Scheduling Algorithm for Heterogeneous Executors for Mimic Clouds[J]. Netinfo Security, 2023, 23(3): 45-55.

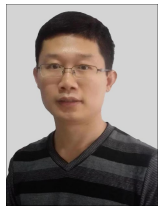
[89] LI W C, ZHANG Z, WANG L Q, et al. The Modeling and Risk Assessment on Redundancy Adjudication of Mimic Defense[J]. Journal of Cyber Security, 2018, 3(5): 64-74.

[90] WU Z Q, ZHANG F, GUO W, et al. A Mimic Arbitration Optimization Method Based on Heterogeneous Degree of Executors [J]. Computer Engineering, 2020, 46(5): 12-18.

[91] GAO Z B, JIANG G R, ZHANG W J, et al. Mimic ruling optimization method based on executive outliers[J]. Application Research of Computers, 2021, 38(7): 2066-2071.

[92] YAO Q, XIONGX L, WANG Y J, et al. Review of moving target defense: an analysis of vulnerability and applications in new scenarios[J]. Control and Decision, 2023, 38(11): 3025-3038.

[93] Deception Defense System[J]. Computer Engineering and Applications, 2022, 58(15): 124-132



HU Hongchao, born in 1982, professor, Ph.D supervisor. His main research interests include cloud computing security and cyber security.

SUI Jiaqi, born in 2000, postgraduate. His main research interests include cyber security and anonymous sommunication.