控制与决策
Control and Decision

移动目标防御综述：脆弱性分析及新场景应用

姚倩, 熊鑫立, 王永杰, 侯冬冬

引用本文:
姚倩,熊鑫立,王永杰,侯冬冬. 移动目标防御综述: 脆弱性分析及新场景应用[J]. 控制与决策, 2023, 38(11): 3025−3038.

在线阅读 View online: https://doi.org/10.13195/j.kzyjc.2022.0584

移动目标防御综述: 脆弱性分析及新场景应用

姚 倩[1,2], 熊鑫立[1,2], 王永杰[1,2†], 侯冬冬[1,2]

(1. 国防科技大学 电子对抗学院，合肥 230037；
2. 国防科技大学 网络空间安全态势感知与评估安徽省重点实验室，合肥 230037)

摘 要: 随着自动化和智能化攻击技术的发展,网络空间安全形势日益严峻,仅靠传统的防御机制已经无法满足当前安全防护的需求. 移动目标防御(MTD)为了扭转网络攻防“易攻难守”的被动局面应运而生,通过增加网络和系统的不确定性、随机性和动态性对抗同类型攻击,通过有效降低其确定性、相似性和静态性降低攻击成功率. 当前,移动目标防御的脆弱性也较少被系统分析,且移动目标防御在新场景下的具体应用较少被具体总结. 鉴于此,首先阐述移动目标防御的产生背景和基础理论;其次,对移动目标防御相关研究进行综述,并分析移动目标防御的脆弱性;接着,总结移动目标防御在物理信息系统、云环境、智能电网和对抗样本防御等新兴领域的应用;最后,对移动目标防御的研究前景进行展望.

关键词: 移动目标防御；脆弱性；新场景应用；动态防御

中图分类号: TP393 **文献标志码:** A

DOI: 10.13195/j.kzyjc.2022.0584

引用格式: 姚倩,熊鑫立,王永杰,等. 移动目标防御综述: 脆弱性分析及新场景应用 [J]. 控制与决策, 2023, 38(11): 3025-3038.

Review of moving target defense: An analysis of vulnerability and applications in new scenarios

YAO Qian[1,2], *XIONG Xin-li*[1,2], *WANG Yong-jie*[1,2†], *HOU Dong-dong*[1,2]

(1. College of Electronic Engineering，National University of Defense Technology，Hefei 230037，China；2. Anhui Province Key Laboratory of Cyberspace Security Situation Awareness and Evaluation，National University of Defense Technology，Hefei 230037，China)

Abstract: With the development of autonomous and intelligent attack technologies, the situation of cybersecurity is becoming increasingly severe, and the traditional defense system can no longer meet the current security requirements. To reverse the passive situation of the network defese, moving target defense (MTD) emerges as the time required, which increases the uncertainty, randomness, and diversity of network and system to resist the same type of attack, and greatly decreases the success rate of attack by effectively reducing its certainty, similarity, and static. At present, the vulnerability of MTD has not been systematically analyzed, and the specific application of MTD in new scenarios has not been summarized. Firstly, the background and basic theoretical knowledge of MTD are illustrated. Secondly, the research related to MTD is reviewed and the vulnerability is summarized. Then, we introduce how MTD can be applied to emerging fields such as cyber-physical systems, cloud environments, smart grids, and the defense of adversarial examples. Finally, the research prospects of MTD are analyzed.

Keywords: moving target defense；vulnerability；the application in new scenarios；dynamic defense

0 引 言

随着云计算、人工智能和区块链等新型技术的发展,网络空间的内涵不断延伸,被称作第五空间,而网络空间安全形势却变得日益复杂、严峻. 确定性、静态性和相似性是网络系统的致命脆弱性,导致网络系统始终处于被动挨打的局面,只能不断提高防御系统的强度来增强安全防护. 但是,在应对越来越自动化和智能化的新型网络攻击时,再健壮的防御系统也经不起攻击者的长期侦察和反复攻击. 因此,仅通过加固防御体系已经无法满足当前网络安全防御的实际需求.

2009 年,“改变游戏规则”的移动目标防御(moving target defense, MTD)[1] 应运而生. MTD 通过增加网络和系统的不确定性、随机性和动态性对抗

收稿日期: 2022-04-11；**录用日期:** 2022-09-03.

†通讯作者. E-mail: wangyongjie17@nudt.edu.cn.

同类型攻击,通过有效降低确定性、相似性和静态性提高系统弹性[2],从而极大地增加了攻击成本,降低攻击成功率,为改变网络攻防对抗的不对称局面提供了新方案. MTD的革命性和创新性在于其一反常态,这是防御策略的大转变和游戏规则的大改变[3]. 随着软件定义网络、虚拟化技术、区块链、物理信息系统和智能电网的不断发展,以及基于机器学习的策略优化方法的不断进步,MTD技术的应用更为广泛.

现有的MTD相关综述[4-6]主要介绍了MTD技术或策略的代表性方法,并未系统地分析MTD的脆弱性,比如:技术固有缺陷的限制、可变换空间大小的限制、软硬件支持不成熟等;现有综述较少深入总结MTD在新场景下的应用. 针对这些问题,本文梳理了当前MTD的脆弱性,为下一步的研究提供参考,同时分析了MTD在新兴领域的具体应用,指明了未来的研究方向.

1 移动目标防御概述

1.1 MTD的基础理论

高级持续性威胁(advanced persistent threat, APT)的发展是促进MTD产生的重要原因之一. APT攻击利用先进的攻击方法对特定目标实施长期的持续性攻击,其特点是针对性强、组织严密、持续时间长、高隐蔽性和间接攻击. APT攻击往往难以提前发现,但造成的后果是灾难性的. MTD通过转换攻击面提供动态的、随机的和适应性的防御,使攻击者探测到的信息全部失效,无法发起有效的APT攻击.

对移动目标防御的研究涉及3个重要概念:移动目标、攻击面和攻击面转换. 在具体介绍移动目标防御之前,先对这几个重要概念加以阐述:

1) 移动目标是指能在多个维度上移动从而降低攻击成功率并增加弹性的系统[7].

2) 攻击面(attack surface, AS)是移动目标防御的重要概念,是指可被攻击者实施攻击的系统资源子集,包括方法(method)、通道(channel)和数据(data),可以表示为

$$\mathrm{AS} = \langle \mathrm{method},\ \mathrm{channel},\ \mathrm{data} \rangle. \tag{1}$$

3) 根据网络中可以被利用的变换面,将MTD技术分为攻击面转换、探索面转换、检测面转换和防御面转换[8]. 攻击面转换(attack surface shifting)是实现移动目标防御的一种重要途径. Jajodia等[3]提出了攻击面转换的定义:给定一个系统t及其运行环境E,记t的旧攻击面为AS_0,新攻击面为AS_n,若存在资源r符合以下两个条件之一,则说明攻击面发生了转换:r属于AS_0但不属于AS_n;r既属于AS_0也属于AS_n,但r在AS_0中的作用大于在AS_n中的作用. 根据此定义可知,攻击面转换能够通过系统资源的转换实现,或者通过变换某一系统资源的作用实现[9].

MTD的目标是在资源有限、保证用户体验的前提下,平衡防御效能与防御代价,有效挫败潜在攻击者. MTD的研究内容包括MTD技术、策略和评估. 支撑MTD技术的设计原则取决于突变元素、突变周期和突变方式. MTD策略主要有随机防御策略、基于博弈论的防御策略和基于机器学习的防御策略. MTD评估主要是评估突变成本和性能消耗,为MTD技术部署和策略优化提供辅助支持. 移动目标防御所涉及的几个重要概念的关系如图1所示.

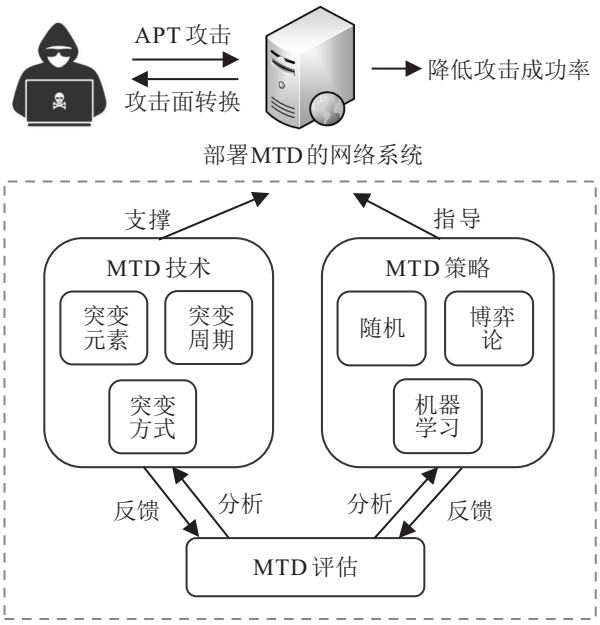

图1 移动目标防御的组成示意图

与移动目标防御关联紧密的有拟态防御(mimic security defense, MSD)[10]和网络欺骗(cyber deception),三者同属于动态防御,都期望改变当前网络“易攻难守”的局面,也都是通过增加不确定性迷惑攻击者以降低攻击成功率. 网络欺骗比移动目标防御具有更强的攻击性,因为网络欺骗会给攻击者提供虚假信息诱导其攻击错误的方向,同时网络欺骗的部署成本和资源消耗一般均低于移动目标防御[11]. 移动目标防御和网络欺骗可以结合使用,首先通过网络欺骗诱导攻击者,然后触发移动目标防御操作. 由于网络欺骗误导攻击者也是动态实现的,一般可以认为网络欺骗是移动目标防御的一部分[12]. 拟态防御由邬江兴院士[10]提出,通过在主动和被动触发条件下,动态、异构、伪随机地运行各种软硬件变体,使硬件执行环境和软件工作状况变得不确定,从

而使攻击者很难利用基于漏洞或后门的攻击链发起攻击. 移动目标防御更倾向于软件层面的防御,而拟态防御则是基于拟态计算的软硬件协同防御.

1.2　MTD的分类方法

MTD技术的设计原则取决于突变元素、突变周期和突变方式,由此对MTD技术进行分类如图2所示. 本节主要对MTD技术加以阐述和分类.

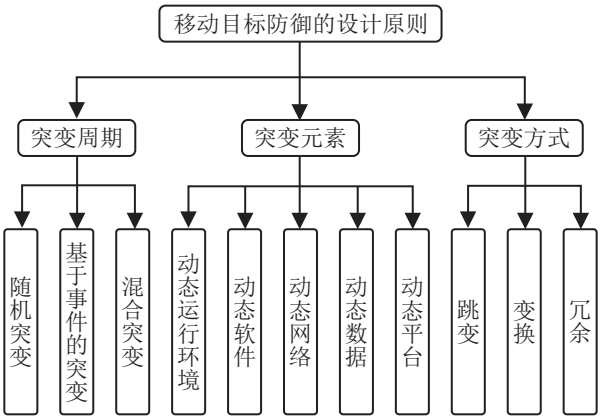

图 2　移动目标防御的设计原则

1.2.1　基于突变元素的分类

突变元素分为网络突变元素和主机突变元素.支撑网络突变的元素有HTML页面元素、Token、IP、端口、网络拓扑、通信协议、MAC地址等,会增加交换机、路由器、DNS或DHCP服务器的工作负载,导致数据包传输时间延长. 主机突变元素有Web服务器、数据库、编程语言、文件信息、数据库信息、软件多样性、虚拟机、指令集、服务版本、地址空间布局等,可能会占用更多的CPU和内存,对应用程序和服务有更大的影响.

根据突变元素,麻省理工学院林肯实验室提出将MTD技术分为5类:动态运行环境、动态软件、动态网络、动态数据和动态平台. 动态运行环境是指操作系统提供的执行环境是动态可变的;动态软件是指应用程序代码是动态可变的;动态网络是指网络的配置和属性是动态可变的;动态数据是指数据的格式、编码方式等是动态变化的;动态平台是指软硬件平台的属性是动态变化的.

1.2.2　基于突变周期的分类

根据突变周期可以将MTD技术分为随机突变、基于事件的突变和混合突变.

随机突变是指在一定时间间隔内产生无规则或周期性的突变. 突变周期需要根据实际情况合理设置,若设置过长则会降低防御有效性,若设置过短则会产生较大的开销. 随机突变的关键是确定最优突变时间. 2021年,Zhang等[13]提出了基于连续时间马尔可夫决策过程(CTMDP)的多阶段攻击动态平台防御模型,根据系统奖励确定最优迁移时间.

基于事件的突变是指当出现攻击迹象或产生安全警报时发生突变,是适应性MTD机制. 为及时发现触发MTD操作的关键事件,研究者们利用机器学习[14-15]和博弈论[16]提出了基于攻击预测的自适应MTD方法.

混合突变[17]将随机突变和基于事件的突变相结合,同时实现主动突变和适应性突变. 2011年,Yih等[18]提出了离线服务器在一定时间间隔内或根据特定事件周期性地替换在线服务器的方法.

1.2.3　基于突变方式的分类

根据突变方式,将MTD技术分为跳变(mutation/hopping)、变换(shuffling)和冗余(redundancy)[19],如图3所示. 跳变是在经过固定或随机的突变周期后,对网络拓扑或系统配置进行扰乱或随机化. 变换是切换以不同方式部署但又提供相同功能的系统组件,使针对某一版本的攻击失效. 冗余是创建多个副本同时提供服务并周期性地重启一个副本.

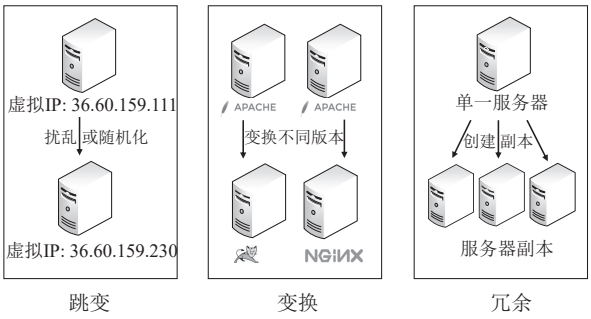

图 3　基于突变方式的MTD技术分类

2　移动目标防御研究进展及其脆弱性分析

2.1　MTD技术及其脆弱性分析

随着MTD研究的不断深入,其被赋予的内涵和所涉及的范围更加广泛,早期提出的基于突变元素的5类分类法不能涵盖所有的突变情况,而基于突变周期的分类法又不够细致,因此本文采用基于突变方式的分类法分析MTD技术,包括跳变、变换和冗余,最后总结MTD技术的脆弱性.

2.1.1　基于跳变的MTD技术

定义 1　跳变(mutation/hopping):在经过固定或随机的突变周期后,对网络拓扑或系统配置进行扰乱或随机化.

本节讨论几种代表性的方法,包括地址空间布局随机化、指令集随机化、数据随机化、IP地址跳变、端

口跳变、虚拟机热迁移、动态网络、和HTML页面元素随机化等.

地址空间布局随机化(address space layout randomization, ASLR): 指内存布局动态变化, 随机化对象包括堆地址、栈基地址、进程环境块地址、线程环境块地址和动态链接库地址. 2002年, Forrest等[20]提出了ASLR以实现计算机系统的多样化. 2012年, Giuffrida等[21]提出了细粒度ASLR以对抗面向内核级的攻击和ROP攻击. 2013年, Snow等[22]通过反复利用内存泄漏动态地映射内存布局, 破坏了细粒度ASLR的有效性, 提出实时代码复用策略. 2013年, Cook[23]提出了内核级ASLR (kernel ASLR, KASLR), 随机化地址支持64位, 扩展内核映像的虚拟内存布局到1 GB. 2016年, Jang等[24]提出了针对KASLR的定时攻击, 利用Intel TSX的硬件特性破解了KASLR.

现有ASLR技术存在以下问题: 1) ASLR只随机化部分组件, 利用未使用ASLR的组件可以进行溢出攻击; 2) ASLR对一些组件地址只在小范围内变换, 通过暴力破解可以获得这些地址; 3) 受限于虚拟内存空间的大小, ASLR在32位的系统中往往不能提供必要的保护; 4) 由内存泄露得到内存布局信息和目标进程状态, 通过得到的堆栈指针绕过ASLR; 5) 覆盖存在溢出函数漏洞的部分返回地址, 使其与基地址的相对距离固定, 找出可利用的跳转指令实施攻击. 针对当前ASLR存在的脆弱性, 可以考虑将ASLR与加密或异或结合使用, 从而提高安全性.

指令集随机化(instruction set randomization, ISR): 防御代码注入型攻击. 若攻击者编写的恶意代码与目标平台使用的指令集不符合, 则恶意代码无法正常执行. 2003年, Kc等[25]创建了随机指令集系统, 若攻击者不知道随机化代码密钥则无法执行恶意代码. 2003年, Barrantes等[26]提出了RISE指令集随机化, 在程序加载到内存时对目标程序全指令采用16位密钥异或加密, 在指令执行时异或解密, 但会产生400%的性能损耗. 2005年, Sovarel等[27]利用蠕虫破解ISR的随机化密钥, 使攻击者需要获得的关键字节数减少到100, 在6 min内破解ISR技术. 2010年, Portokalidis等[28]对ELF文件程序实现了基于动态二进制分析平台Pin的ISR技术, 前提是ELF格式文件数据和指令严格分离. 2013年, Papadogiannakis等[29]提出了支持ISR的硬件和操作系统的体系架构ASIST, 同时降低了性能消耗.

目前, ISR技术存在以下脆弱性: 1) ISR技术需要密钥异或加解密、共享库和随机化指令集软件的支持, 编码实现困难; 2) ISR技术基于二进制转换工具实现, 运行时需要使用额外软件解析指令集, 产生较大的性能开销; 3) ISR需要同时更改操作系统和硬件平台, 实际部署困难; 4) ISR技术只能防御代码注入攻击, 无法抵御代码复用攻击; 5) 现有ISR技术无法有效防御内核漏洞攻击; 6) 遭受密钥暴力破解攻击, 利用蠕虫病毒等降低破解随机化密钥的所需次数.

数据随机化(data space randomization, DSR): 使内存中的数据随机化以防止信息泄露攻击. DSR根据指令指向的对象将指令操作数划分为等价类, 并为每个等价类分配一个随机掩码, 在执行写内存时对写入的值进行异或加密, 执行读内存时对读取的值进行异或解密, 确保数据在内存中加密存储. 2008年, Bhatkar等[30]提出了数据随机化, 以较小的开销有效防御DOP (data oriented programming)攻击[31]和内存泄漏攻击. 2020年, Rajasekaran等[32]提出了CoDARR机制, 能够在固定周期内或根据需求动态地调整随机掩码, 并通过内存泄漏攻击和旁路攻击验证了所提出方案的有效性.

IP地址跳变: 指虚拟IP在固定周期内或随机进行跳变, 从而使攻击者无法溯源到真正的IP地址. 2014年, Carroll等[33]基于URN模型, 理论分析了IP地址跳变的有效性, 发现IP地址跳变在脆弱主机很少的网络中具有更好的保护效果. 2018年, Sharma等[34]在软件定义网络中使用随机虚拟IP地址FRVM, 能够使攻击者探测到的信息失效. IP跳变、端口跳变或创建服务器副本等MTD技术可以抵御DDoS攻击, 由于创建服务器副本的维护成本较高, 2021年Feng等[35]在DNS服务器上实现IP地址快速跳变来迷惑攻击者, 从而抵御DDoS攻击.

端口跳变: 指服务端口跳变来隐藏服务标志的方法. 2012年, 针对端口跳变如果丢失同步确认则可能遭受DDoS攻击的问题, Fu等[36]提出了BIGWHEEL算法, 以一种无需同步的方式使每个应用服务器与多个应用服务器进行通信. 2020年, Navas等[37]将UDP端口跳变应用于物联网系统.

虚拟机热迁移: 指虚拟机的动态迁移, 即完整保存虚拟机的运行状态, 同时快速恢复到原有硬件平台或不同硬件平台上. 2011年, Danev等[38]针对私有云的虚拟机安全迁移问题, 将可信计算集成到虚拟计算环境中, 提出了虚拟可信平台模块迁移协议VM-vTPM. 2017年, Rodrigues等[39]通过虚拟机迁移和传输功率控制, 在边缘云计算中实现了最小服务延迟. 2021年, Duong-Ba等[40]提出了多级连接虚拟

机放置与迁移(MJPM)算法,使数据中心的资源使用和功耗最小化. 然而,容器或虚拟机热迁移技术会消耗一定的资源,间接导致云服务的性能下降,可以考虑轻量级的微型虚拟机热迁移技术.

动态网络:指网络配置信息的动态变化. 2014 年 Kampanakis 等[41] 在 SDN 框架上实现了攻击面的动态转换,由 SDN 控制器得到网络状态,再按照固定周期随机改变 IP 地址、路由等,通过分析网络和配置信息得到实时数据,以对当前所面临的威胁和攻击进行评估. 2020 年, Yoon 等[42] 提出处于攻击路径上的主机网络配置发生跳变的方法,开发了评估网络脆弱性和网络拓扑结构的分层攻击图模型,该模型可以决策 MTD 的变换频率.

HTML 页面元素随机化:指 HTML 页面元素在一定时间内发生变化,防止恶意爬虫. 2013 年, Vikram 等[43] 提出了 NOMAD,通过在 Web 应用中随机化 HTML 页面可输入元素的标签属性,以减少黑帽搜索引擎优化工具攻击.

综上所述,跳变通过扰乱或混淆网路拓扑或系统配置来实现,相对于变换和冗余,跳变的资源消耗较少,但是网络层 MTD 技术将直接导致 Web 服务质量下降,并影响服务之间的通信,因此跳变的可靠性和稳定性都比较差;另一方面,即使牺牲了较高的防御成本来增加跳变频率,跳变的方式依然会受到技术或组件固有缺陷的影响,比如网络配置本身就存在漏洞,采用动态网络也无法规避该问题.

2.1.2　基于变换的 MTD 技术

定义 2　变换(shuffling):切换以不同方式部署但又提供相同功能的系统组件,使针对某一版本的攻击失效.

代表性的变换方式主要有:编程语言转换、动态平台和动态软件等,下面分别介绍.

编程语言转换:指转换程序或应用的开发语言以抵御代码注入攻击和 SQL 注入攻击. 2015 年, Taguinod 等[44] 分析了在 Web 不同层部署 MTD 的可能性,然后在不影响或中断系统功能的前提下,将转换编程语言应用于 Web 应用程序以抵御 Web 利用漏洞,但这种方法会产生实时更新和同步多种编程语言的维护成本.

动态平台:指操作系统或硬件平台产生动态变化. 2012 年, Okhravi 等[45] 设计了可信动态逻辑异构系统(trusted dynamic logical heterogeneity system, TALENT),能够动态地变换硬件平台和操作系统,使对于特定平台漏洞的攻击全部失效. 2021 年, Zhang 等[13] 提出了基于连续时间马尔可夫决策过程(CTMDP)的多阶段攻击动态平台防御模型,根据系统奖励确定最优迁移时间.

动态软件:指应用程序或代码进行动态变化. 2011 年, Azab 等[46] 基于生物学的启发,提出了动态应用程序和代码变体的架构 ChameleonSoft,提供自适应、态势感知的动态防御.

综上所述,变换的成本代价相对跳变较高,相对冗余较低. 变换可以与跳变相结合,如果只使用跳变则需要增加更高的跳变频率以保证安全性,而当结合使用跳变和冗余时,在降低跳变频率的情况下,也可以达到较高的防御有效性. 然而,变换的有效性受限于可变换的数量,以动态平台为例,若只有两个版本的平台可供变换,则其有效性是受限制的.

2.1.3　基于冗余的 MTD 技术

定义 3　冗余(redundancy):提供服务器或网络组件的多个副本,可以在网络层或应用层提供相同的功能.

服务器副本:指创建服务器副本,在当前服务器受到攻击时逐步转移到新的服务器上以减少损失. 2010 年, Roeder 等[47] 提出了主动模糊(proactive obfuscation),通过为服务器创建多个副本并使用可执行程序周期性重启一个新副本来对抗攻击,但是固定周期性重启存在新服务器容易被定位的缺陷. 2014 年, Jia 等[48] 针对冗余技术容易被攻击者重新定位新服务器的情况,首先使用跳变将良性客户机分配到新的副本服务器,然后跟踪分配以及新副本受攻击的情况,从而快速识别恶意攻击者.

综上所述,相比跳变和变换,冗余具有更高的可靠性和服务可用性,但是存在较大的成本代价和资源消耗,创建副本需要较高的人力与资金成本,实时备份和更新数据都需要较高的维护成本,且若操作不当则存在增大攻击面的风险.

2.1.4　MTD 技术的脆弱性

综上所述,跳变的方式资源消耗较少,但是其可靠性和稳定性都比较差,网络层 MTD 技术将导致 Web 服务质量下降. 此外,跳变还会受到技术或组件固有缺陷的影响. 变换可以与跳变相结合,以较低的资源损耗达到较好的防御效果,而变换的有效性显著受限于可变换的数量. 冗余具有更高的可靠性和服务可用性,但是存在较大的成本代价. 现有 MTD 技术的分析总结如表 1 所示.

表1 现有移动目标防御技术的分析总结

分类	典型技术	相关文献	防御效果	脆弱性分析	技术特点
跳变	地址空间布局随机化	[20-24]	抵御部分缓冲区溢出攻击	只随机化部分组件; 小范围内跳变; 受限于内存空间的大小无法抵御内存泄漏攻击; 受溢出函数漏洞的影响	优点: 使攻击者收集到的信息失效; 资源消耗相对较少; 缺点: 服务不稳定, 可靠性差; 受到固有技术或组件缺陷的影响
	指令集随机化	[25-29]	抵御部分代码注入型攻击和SQL注入攻击	编码困难; 性能消耗较大; 硬件支持不成熟; 无法抵御代码复用攻击和内核漏洞攻击; 可能遭受密钥暴力破解攻击	
	数据随机化	[30-32]	抵御DOP攻击和部分内存泄漏攻击	可能遭受随机掩码暴力破解攻击; 无法抵御溢出攻击	
	IP地址跳变	[33-35]	使攻击者无法锁定真正的IP地址, 一定程度上抵御DDoS攻击	可靠性和稳定性较差; 受限于可跳变的数量	
	端口跳变	[36-37]	使攻击者丢失攻击目标, 一定程度上抵御DDoS攻击	服务不稳定; 服务器和客户机的同步问题	
	虚拟机热迁移	[38-40]	实现云安全	造成服务延迟; 产生额外开销	
	动态网络	[41-42]	网络配置随机化, 迷惑攻击者	影响网络服务间的通信, 服务质量下降	
	HTML元素随机化	[43]	抵御恶意爬虫	数据库维护和同步问题	
变换	编程语言转换	[44]	抵御代码和SQL注入攻击	程序运行稳定性差; 实时同步代码的维护成本高.	优点: 使针对某一版本的攻击失效; 与跳变相结合可达到更好的效果; 缺点: 资源消耗较大; 受限于可变换的数量
	动态平台	[13, 45]	使对于特定平台的漏洞攻击失效	随机迁移产生的开销较大; 受限于可变换的平台数量	
	动态软件	[46]	使针对某个版本软件的攻击失效	受限于可变换的版本数量; 开销更大	
冗余	服务器副本	[47-48]	更高的可靠性和服务可用性; 一定程度上抵御DDoS攻击	实时备份和更新数据需要较高的维护成本; 如果操作不当则有增大攻击面的风险	优点: 高可靠性和服务可用性; 缺点: 更高的维护成本和开销

2.2 MTD评估及其脆弱性分析

2.2.1 MTD的评估方法

一般而言, 在进行MTD策略优化前需要先评估MTD技术的性能和耗费. MTD技术的效能评估需要量化攻击面的变化, 评估突变成本, 考虑有效性、服务可用性、成本代价和资源损耗. 2016年, Hong等[19]采用比普通攻击图更加灵活和可扩展的分层攻击代表模型HARM以评估MTD技术的有效性. 2017年, Bopche等[49]利用最大公共子图和图编辑距离度量动态网络攻击面的时间变化. 2017年, 为实现对MTD成本和收益的实时检测和动态度量, 雷程等[50]提出了基于分层资源图的变点检测和标准化度量的效能评估方法. 2018年, Hong等[51]考虑到不同MTD技术变化范围不同, 将MTD技术结合到基于时间图的图形安全模型中, 评估了拓扑跳变和软件变换的有效性. 2019年, 针对较大规模网络下对多层次MTD技术的有效性评估问题, 熊鑫立等[52]提出基于系统攻击面变化参数序列的评估模型, 分析了攻击状态与系统攻击面变化参数间的联系. 针对攻防过程描述不准确导致评估存在偏差的问题, Xiong等[53]基于系统视图扩展攻击面模型对攻防交互行为进行评估, 提出SAS模型分析攻防行为对系统资源的影响, 根据非齐次隐马尔可夫模型及其观察序列, 利用部分维特比算法确定攻击状态的可能序列. 2020年, Sharma

等[54]针对基于SDN的MTD技术,从三方面实时、动态、自适应地评估MTD的变化,包括基于网络和IP地址跳变的度量、基于攻击路径的度量和基于攻击阶段成功率的度量. 2021年, Gao等[55]根据探测到的地址数、网络规模、网络结构和地址转换频率等量化了MTD技术和网络欺骗的防御性能,基于Urn模型评估两种方法的防御效能.

2.2.2　MTD评估的脆弱性

当前,MTD效能评估的方法主要有攻防实验、模拟仿真、数学推理和综合方法[51],针对攻防实验和模拟仿真的应用场景受限,而数学推理又存在抽象、结果有偏差的问题,可以考虑采用数学推理与实验验证相结合的综合方法. 针对评估标准不统一的问题,可以研究如何构建统一的量化标准. 针对MTD不同技术有不同变化范围和使用场景的问题,可以研究如何更加精确地评估MTD技术或策略.

MTD的效能评估方法也存在脆弱性: 1) MTD的效能评估一般在系统运行时采用先验知识进行评估,不能实时反映MTD系统的效能; 2) 为保证MTD系统顺利运行,需要在资源受限的情况下进行MTD的效能评估,导致所能采用的MTD效能评估方法的复杂度一般不会很高; 3) MTD的效能评估基于对攻击者的建模,由于建模的抽象程度不同,导致MTD评估的准确性受到影响; 4) MTD效能评估的准确性与MTD策略的选取息息相关,如果MTD效能评估得不准确,则会使制定的MTD策略与预期效果产生偏差,未达到设想的防御效果,从而导致MTD策略的脆弱性问题.

2.3　MTD策略及其脆弱性分析

MTD策略主要是研究在不同攻防对抗场景中选择恰当的突变元素和突变方式以及确定合适的突变周期,从而为防御者提供有效且开销较小的策略. MTD策略的研究也是当前一个研究热点,MTD策略是否达到预期效果,需要对其进行效能评估,根据反馈的评估效果进一步优化MTD策略. MTD策略和MTD评估是相辅相成的,本节首先介绍MTD的效能评估方法;然后介绍MTD策略,包括随机防御策略选择、基于博弈论的防御策略和基于机器学习的防御策略等;最后总结MTD策略的脆弱性.

2.3.1　随机防御策略

随机策略是指产生随机突变的策略. 2014年, Thompson等[56]提出MORE MTD系统,设置了多个虚拟机提供相同的服务,在未被攻击时按照固定周期进行改变,当检测到攻击后随机选择另一个虚拟机代替当前虚拟机,使攻击者收集的信息失效. 2016年, Chowdhary等[57]使用SDN控制器通过扩展攻击图自动化地评估攻击场景,然后实时随机化网络配置. 2016年, Aydeger等[58]提出了基于SDN的随机路由选择方案,以避免报文转发过程中出现拥塞链路,从而抵御新型DDoS攻击CrossFire. 2021年,徐潇雨等[59]提出了软件定义网络中基于深度确定性策略梯度(DDPG)的随机路由策略,随机策略部署简单,但存在开销较大的问题,如何设置最佳的突变点是亟待解决的问题,且随机防御策略不适用于需要隐蔽性MTD技术的特定场景,如面向电网的虚假数据注入攻击.

2.3.2　基于博弈论的防御策略

网络攻防中的目标对立性、关系非合作性和策略依存性与博弈论的特征一致[60],基于博弈论的防御策略从博弈角度就攻防之间的关系进行建模. 2017年, Feng等[61]提出了攻击者为领袖、防御者为追随者的贝叶斯斯坦科尔伯格博弈模型,为防御者设计信号策略,利用MTD影响攻击者行为得到信号有用性的条件. 2018年, Lei等[62]将转移攻击面与改变扫描面作为防御者动作并建立了多阶段对抗模型,依据马尔科夫过程在每个阶段选择防御回报最大的动作作为防御策略. 2019年, Zhou等[63]利用多目标马尔可夫决策过程模拟攻防之间的相互作用,结合端口跳变、IP跳变和虚拟机迁移抵御DDoS攻击. 2020年, Sengupta等[64]建立了不完全信息贝叶斯Stackelberg马尔科夫博弈模型(BSMGs),应用多智能体强化学习(BSS-Q)表征攻击类型和MTD系统的细微差别. 2020年,陈子涵等[65]考虑用户对网络攻防的影响,提出了基于Stackelberg-Markov非对等三方博弈模型的MTD策略. 2021年,针对现有防御存在持续决策实时性不强的问题, Tan等[66]提出基于侦查-攻击-检测攻击面的多维转换MTD模型,分析了MTD攻防博弈和时空策略的特点以及网络攻防的连续过程,建立了MTD时空决策模型. 为了更贴合持续的、动态的应用场景,研究者们开始关注多阶段进化、演化博弈和微分博弈等. 演化博弈借鉴生物的思想,将演化与博弈论相结合,更加贴合动态的攻防场景. 而微分博弈是指基于网络攻防的连续时间过程建立博弈论模型. 然而,基于博弈论的MTD策略设计得越来越复杂,使得优化算法的复杂度也随之增加.

2.3.3　基于机器学习的防御策略

基于机器学习的防御策略是新兴的研究点,MTD策略存在多层次、优化算法复杂度高等问题,

基于机器学习的方法可以很好地进行解决. 2020年, 熊鑫立等[67]针对多层次、多参数变化的MTD策略优化问题, 从系统角度分析MTD技术的不同参数的影响, 构建系统正常服务和重配置过程模型, 提出了基于马尔可夫决策过程的MTD策略优化方法, 并使用Q-learning算法得到优化策略集合. 2020年, Eghtesad等[68]建立了基于MTD的多智能体部分可观测马尔科夫决策过程(POMDP)模型, 利用多智能体强化学习算法求解两层非零和博弈问题以寻求最优MTD策略. 2020年, Sengupta等[69]提出了自适应MTD策略, 通过多智能体强化学习求解贝叶斯Stackelberg马尔可夫博弈模型. 2021年, Gao等[70]提出了基于强化学习的自适应MTD策略对抗DDoS攻击, 根据环境状态的改变自适应调整防御策略. 基于机器学习的防御策略解决了优化算法复杂度较高的问题, 将博弈论与机器学习相结合是MTD策略的发展趋势.

2.3.4 MTD策略的脆弱性

综合当前研究现状可以发现, MTD策略的研究从完全信息向不完全信息发展, 从攻防双方完全理性到有限理性发展, 从攻防双方到攻-防-用户的三方博弈, 从静态防御向动态、主动、适应性防御发展, 从随机策略到博弈论再到基于机器学习的策略发展.

当前MTD策略也存在脆弱性: 随机策略开销较大, 不适用于隐蔽性MTD技术的特定场景; 博弈论的算法复杂度高, 现有方法基于先验知识, 不满足实时性要求; 基于机器学习的方法可能遭受动态目标攻击(moving target attack, MTA). MTA攻击是指攻击者通过故意隐藏其攻击能力来诱导MTD降低系统的随机性、动态性和不确定性, 从而相对提高攻击的成功率. 尽管对于纯随机策略和固定策略, MTA无法有效提高攻击成功率, 但是当MTD采用某种策略优化方法时, 针对其对系统可用性的要求, MTA可以适应性地调整攻击强度, 诱导MTD策略降低重配置能力. 同时, MTA注重攻击的智能性, 不断发展的人工智能技术和数据分析能力, 都为MTA的实现提供了有效的技术手段. 此外, MTD策略需要在安全性与可用性之间取得折中, 为保证系统服务的可用性和可靠性, 兼顾资源消耗, 都会不可避免地牺牲一定的安全性.

3 新场景下移动目标防御技术的应用

将MTD应用于物理信息系统、云环境、智能电网和对抗样本防御等新兴领域是当前的研究热点. 物理信息系统的资源受限, 不支持复杂的加密算法; 云环境存储着大量软件数据, 需要高可靠性和高稳定性的支持, 且云环境能够根据需要创建副本, 进行虚拟机热迁移等; 智能电网深度集成了新一代信息技术, 专业性极强; 对抗样本是针对静态的特定目标反复测试而生成的. 针对这些新型应用场景, 低耗费、轻量化、自动化和动态化的MTD技术有着非常广阔的发展空间. 本节将讨论MTD在物理信息系统、云环境、智能电网和对抗样本防御中的具体应用.

3.1 物理信息系统中的MTD技术

物理信息系统(cyber-physical systems, CPS)是融合了控制、通信和计算的多维度智能系统, 当前物理信息系统应用在人类生活的各个方面, 而物理信息系统的安全措施却远落后于互联网, 将MTD技术应用于物理信息系统是近几年的研究热点. 2019年, Nizzi等[71]提出了IP和MAC地址随机化的方法HMAC, 并将其部署于物理信息系统中. 2020年, Navas等[37]提出了IANVS架构, 将UDP端口跳变应用于物理信息系统. 2020年, Ge等[72]将MTD与网络欺骗相结合从而实现物理信息系统的主动防御, 采用固定、随机、自适应和混合策略分析何时变换物理信息系统的网络拓扑, 并且对欺骗效能、服务可用性、资源成本的平衡进行了分析.

3.2 云环境下的MTD技术

云环境能够通过互联网提供动态易扩展的虚拟化资源, 而许多云基础设施的配置是静态和同构的, MTD可以提高云服务的动态性和不确定性. 2014年, Peng等[73]提出了基于异构动态攻击面的MTD策略以实现云安全. 2016年, Azab等[74]针对云计算的旁路攻击, 提出了实时随机迁移的轻量级防御方法MIGRATE. 2018年, Sengupta等[75]针对在云端部署较多入侵检测系统(IDS)会影响系统性能的问题, 提出了在每一个周期内策略性地改变IDS布局配置的方法以减少IDS的部署数量, 将管理员和攻击者构建为Stackelberg博弈模型来确定IDS的部署数量. 2019年, Jin等[76]提出了自动化感知容器云环境并动态更新的框架DSEOM, 可以快速评估MTD的有效性, 动态优化MTD策略.

3.3 智能电网中的MTD技术

针对电网的虚假数据注入攻击(false data injection attack, FDIA)是指通过恶意篡改电力信息系统中的测量和控制数据, 对电力业务实施网络攻击[77], 应用MTD技术扰动传输线电抗器可以抵御FDI攻击. 2020年, Lakshminarayana等[78]提出了MTD技术有效抵御FDI攻击并保持隐蔽性的条件和启发式MTD干扰电抗的方法, 尽可能平衡MTD技

术的探测能力和所需成本. 2020 年, Higgins 等[79] 通过 T-SNE 降维和 DBSCAN 聚类算法, 将电流观测数据聚类成相关联的拓扑轮廓, 计算出 FDI 攻击的混合矩阵, 提出了将 MTD 技术与物理水印相结合的方法. 2020 年, 张镇勇等[80] 提出了以相同比值扰动环中所有输电线路的电纳值来实现隐蔽性 MTD, 同时证明了在对抗 FDI 攻击时实现完备性 MTD 的要求: 输电线路数要大于等于系统状态数量的两倍; 至少有 n 条输电线路的阻抗被扰动, 且要覆盖系统中所有节点. 2021 年, Lakshminarayana 等[81] 为分布式柔性交流输电系统 (D-FACTS) 设备划分了防御者能够识别任意链路存在协同网络物理攻击 (CCPAs) 的子集, 建立零和博弈以确定对干扰攻击者的最佳链路子集. 2021 年, Liu 等[82] 基于图论技术, 分析了在分布式柔性交流传输系统 (D-FACTS) 布局中应用隐蔽 MTD 技术的充分条件. 然而, 攻击者在实施 FDI 攻击时会先检测是否部署了 MTD, 当随机扰动输电线路参数时很容易被攻击者发现, 隐蔽性极差; 而使攻击者完全无法检测实现隐蔽性 MTD, 可用性并不可观. 因此, 隐蔽性和可用性的平衡问题是在智能电网中应用 MTD 的难题.

3.4　对抗样本防御中的 MTD 技术

针对机器学习模型的对抗样本攻击是一个研究热点, 对抗样本攻击通常是攻击者对一个固定目标不断地重复探测直到其构造出对抗样本的过程, 采用 MTD 技术可以防御对抗样本. 2019 年, Roy 等[83] 将攻击过程建模为攻防 Stackelberg 博弈模型, 提出了一种切换机器学习算法的方案来抵御有限理性攻击者的对抗攻击. 2020 年, Wang 等[84] 针对深度神经网络的恶意输入问题, 提出了一个异构、可选择、适应性的安全框架 MTDNNF, 以改进恶意输入, 提高系统安全性. 2021 年, Amich 等[85] 提出了 Morphence 模型, 通过部署一个具有 n 个模型的模型池并设置调度策略定期改变模型的决策函数, 当被攻击时选择一个最适合的模型抵御重复或相关联的对抗样本攻击. 然而, 当前防御对抗样本的 MTD 技术受限于可变换的算法或函数的数量, 当攻击者为可变换的几种算法都精心设计出对抗样本时, 便可绕过 MTD 技术.

3.5　其他新场景中的 MTD 技术

除了以上提到的 CPS、云环境、智能电网和对抗样本防御, MTD 也能够应用于其他新场景.

1) 区块链. 2020 年, 针对传统虚拟机或容器热迁移有可能被路由跟踪的问题, Magdy 等[86] 提出了基于区块链的动态路由机制, 使联邦云环境中的虚拟机或容器实现匿名实时热迁移. 2021 年, He 等[87] 提出了在物联网设备中对 IP 地址使用随机安全参数加密、客户端采用公钥加密和区块链技术进行身份认证的方法, 以阻断物联网的 DDoS 攻击.

2) 车载控制器局域网 (controller area network, CAN). 车载网络不提供访问控制、身份验证, 无法抵御攻击者侦察, 其静态配置很容易使攻击者探测到有用的攻击信息. 2019 年, Woo 等[88] 提出了一种基于车载网络 ID 的跳变技术, 旨在增加攻击者分析车载网络数据帧的成本代价.

3) 防范勒索软件. 2019 年, Lee 等[89] 提出了随机更改勒索软件试图加密的文件扩展名来抵御勒索软件攻击的方法, 从而保护有价值的文件.

当前, MTD 被应用于各种新场景, 在某种程度上, 新场景下使用 MTD 对于创新方案方法有着极大的指导意义, 但也面临着一些挑战, 比如: 物理信息系统的资源受限, 云环境会遭受旁路攻击, 智能电网中需要平衡 MTD 技术的隐蔽性和可用性, 对抗样本防御存在受限于可变换的算法或函数, 车载控制器局域网缺少访问控制和身份认证, 其静态配置很容易被攻击者探测. 新场景下应用 MTD 技术面临的挑战和未来的研究方向如表 2 所示.

表 2　新场景下应用 MTD 技术面临的挑战和未来的研究方向

新场景	相关文献	面临的挑战	未来的研究方向
物理信息系统	[37,71-72]	资源受限, 不支持复杂加密	资源受限条件下的 MTD 技术
云环境	[73-76]	遭受旁路攻击; 服务质量下降	隐蔽性 MTD 技术以防止虚拟机热迁移时被跟踪路由信息; 轻量级 MTD 技术以减少资源损耗、提高服务可用性
智能电网	[77-82]	随机扰动无法抵御 FDI 攻击; 部署有效的 MTD 技术需要极高的专业领域知识	平衡 MTD 技术隐蔽性和可用性的新方案
对抗样本防御	[83-85]	受限于可变换的算法或函数	将 MTD 技术与数字水印技术相结合, 提高模型鲁棒性
区块链	[86-87]	MTD 技术的随机化参数可能被攻击者暴破	对 MTD 的随机化参数进行加密, 防止攻击者绕过 MTD 技术
车载控制器局域网	[88]	没有访问控制、身份验证, 无法阻挠攻击者侦察	将 MTD 技术和区块链技术相结合, 融入身份认证机制

4 未来的研究方向

MTD提供动态的、适应性的主动防御,增加了网络和系统的随机性和不确定性,为扭转“易攻难守”的网络态势提供了新思路. 根据当前研究现状,下一步值得关注的研究方向有:MTD脆弱性分析与完善,新场景下MTD技术的改进与发展,MTD准确评估与自适应策略和MTD大规模敏捷部署方法等.

4.1 MTD脆弱性分析与完善

MTD具有非常广泛的应用前景,但并非坚不可摧,在一个脆弱的网络中部署MTD系统也不意味着一劳永逸. 比如:32位的ASLR技术已经不能提供必要的保护,指令集随机化技术存在运行内存占用较高的问题,网络层MTD技术带来的服务质量下降问题,虚拟机热迁移带来的服务延迟的问题,动态平台技术受限于可变换的数量,冗余的方法会带来很大的额外开销和数据维护问题,MTD评估存在不能实时反映MTD系统效能、复杂度不高、准确性受限等问题,MTD策略为保证服务可用性而不可避免地存在安全隐患问题. 针对MTD的脆弱性研究相应的规避方法是一个重要的研究方向.

4.2 新场景下MTD技术的改进与发展

MTD并不是某种特定的技术,而是一种设计指导思想,具有非常重要的应用价值. 当前,MTD应用于互联网已有大量研究成果,而将MTD应用于安全防护相对较弱的物理信息系统、云环境、智能电网、对抗样本防御、车载控制器局域网等领域仍有广阔的发展空间. 物理信息系统的资源受限,可以考虑低耗费、轻量化的MTD技术;云环境存储着大量软件数据,需要高可靠性和高稳定性的支持,且云环境能够根据需要创建副本、进行虚拟机热迁移等,可以考虑构建自动化配置的MTD技术;智能电网深度集成应用新一代信息技术,专业性极强,面向针对电网的FDI攻击可以考虑采用机器学习的方法区分真实数据和虚假数据,再应用MTD技术抵御FDI攻击;MTD防御对抗样本能够起到一定的积极作用,但其受限于可变换的算法或函数的数量,将MTD技术与数字水印技术相结合,可以提高模型鲁棒性;车载控制器局域网没有身份认证且配置静态,容易被窃听或篡改,可以将MTD技术与区块链技术相结合.

4.3 MTD准确评估与自适应策略优化方法

MTD效能的准确评估和自适应策略优化方法是一个相辅相成的问题. MTD实时准确评估能促进生成自适应策略优化方法,而自适应策略优化方法能够不断反馈给MTD系统,促使实时准确地评估MTD. 然而,在实际部署MTD策略时,要考虑其有效性、服务可用性、成本代价和资源损耗. MTD技术范围广泛、动态持续,具有不同的变化范围,为MTD的评估与策略优化带来极大的挑战. 只有准确评估MTD的效能和耗费,才能确定在某一网络中是否应该部署MTD技术、部署哪一种MTD技术,才能发现MTD技术的改进方向,才能确定MTD策略是否合理. 同时,根据网络的实时态势和MTD评估结果自适应地进行MTD策略优化,使MTD的优化策略能够尽可能地提高防御效果. 当前,基于博弈论的MTD防御策略被广泛研究,然而传统博弈论方法基于先验知识,不能很好地满足实时性的要求,且算法复杂度高,求解困难. 针对MTD技术具有动态变化、持续性变化的特点,可以考虑演化博弈论或微分博弈. 针对MTD准确评估和优化策略求解困难的问题,可以考虑采用机器学习.

4.4 MTD技术的大规模敏捷部署方法

当前,MTD已经能够实际部署在单一或小规模数量的主机上,如ASLR已经能够应用在Windows、Linux等平台. 而仅在小规模范围内部署,其防御效果是非常有限的,攻击者仍然能够针对网络攻击路径中的薄弱环节实施攻击,但是大规模范围内部署MTD存在一些现实问题仍未解决. 网络层MTD技术将直接导致Web服务质量下降,并影响合法用户与服务之间的通信;容器或虚拟机热迁移等MTD技术会消耗一定的系统资源,从而间接导致云服务的性能下降. 总体而言,大规模部署MTD会产生性能下降和服务延迟等,甚至会出现服务不可用的问题. 这些问题都成为MTD大规模部署的阻碍. 而实施轻量化的、敏捷的微型MTD技术可以降低性能损耗,提高服务可用性,有望解决MTD技术的大规模敏捷部署问题,这是一个有前景的研究方向.

5 结 语

随着网络空间的不断发展,新型网络攻击也层出不穷,传统静态防御技术往往不能满足实际需求,为改变传统防御技术“易攻难守”的被动局面,动态的、随机的、不确定的移动目标防御应运而生. 本文首先介绍了MTD的基本思想,分析了MTD的基本问题,提出了MTD的分类方法;然后,基于突变方式的分类法,较全面地分析了MTD的技术、策略和评估方法,着重讨论了MTD的脆弱性,MTD技术存在服务不稳定、可靠性差、技术或组件固有缺陷、可变换的空间大小、更高的维护成本和开销等脆弱性,MTD评估存在不能实时反映MTD系统效能,复杂度不高,准确性

受限等问题, MTD 策略为保证系统服务的可用性和可靠性, 都会不可避免地牺牲一定的安全性, 同时受到 MTA 的威胁; 接着分析了 MTD 在物理信息系统、云环境、智能电网和对抗样本防御等新型场景中的实际应用, 针对这些场景, 低耗费、轻量化、自动化、自适应的 MTD 技术有着非常广阔的发展空间; 最后提出了 MTD 未来的研究方向.

MTD 是一个富有前景的研究领域, MTD 提供了动态、适应性防御的新思路, 当前 MTD 已经有实际应用, 但是典型 MTD 系统存在的脆弱性始终是令人担忧的, 进一步完善典型 MTD 的脆弱性有着重要的意义. 同时, MTD 并非仅限于提高互联网网络的弹性, 它还能够适用于多种新型应用场景. 在某种程度上, 新场景下使用 MTD 对于创新方案方法有着极大的指导意义. 通过本文的工作, 可以进一步指导 MTD 的发展.

参考文献(References)

[1] Nitrd C I. Cybersecurity game-change research and development recommendations[Z]. 2010.

[2] 王永杰. 网络动态防御技术发展概况研究[J]. 保密科学技术, 2020(6): 9-14.
(Wang Y J. Research on the development of dynamic defense technology[J]. Secrecy Science and Technology, 2020(6): 9-14.)

[3] Jajodia S, Ghosh A K, Subrahmanian V S. Moving target defense II[M]. Berlin: Springer Science & Business Media, 2012: 4-5.

[4] 周余阳, 程光, 郭春生, 等. 移动目标防御的攻击面动态转移技术研究综述[J]. 软件学报, 2018, 29(9): 2799-2820.
(Zhou Y Y, Cheng G, Guo C S, et al. Survey on attack surface dynamic transfer technology based on moving target defense[J]. Journal of Software, 2018, 29(9): 2799-2820.)

[5] 蔡桂林, 王宝生, 王天佐, 等. 移动目标防御技术研究进展[J]. 计算机研究与发展, 2016, 53(5): 968-987.
(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.)

[6] 樊琳娜, 马宇峰, 黄河, 等. 移动目标防御技术研究综述[J]. 中国电子科学研究院学报, 2017, 12(2): 209-214.
(Fan L N, Ma Y F, Huang H, et al. The research summary of moving target defense technology[J]. Journal of China Academy of Electronics and Information Technology, 2017, 12(2): 209-214.)

[7] The White House National Security Council. Cybersecurity progress after president obama's address[R]. New York, 2012.

[8] 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.

[9] 蔡桂林. 移动目标防御技术若干关键问题研究[D]. 长沙: 国防科学技术大学, 2016.
(Cai G L. Research on some key issues for moving target defense[D]. Changsha: National University of Defense Technology, 2016.)

[10] 邬江兴. 网络空间拟态安全防御[J]. 保密科学技术, 2014(10): 4-9.
(Wu J X. Network mimicry security defense[J]. Secrecy Science and Technology, 2014(10): 4-9.)

[11] 王永杰, 高春刚. 基于蜜罐的欺骗式主动防御的发展与演进[J]. 保密科学技术, 2021(2): 10-14.
(Wang Y J, Gao C G. Development and evolution of deceptive active defense based on honeypot[J]. Secrecy Science and Technology, 2021(2): 10-14.)

[12] 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.

[13] Zhang Y P, Chang X L, Mišić J, et al. Cost-effective migration-based dynamic platform defense technique: A CTMDP approach[J]. Peer-to-Peer Networking and Applications, 2021, 14(3): 1207-1217.

[14] Colbaugh R, Glass K. Predictability-oriented defense against adaptive adversaries[C]. IEEE International Conference on Systems, Man, and Cybernetics. Seoul, 2012: 2721-2727.

[15] Nanda S, Zafari F, DeCusatis C, et al. Predicting network attack patterns in SDN using machine learning approach[C]. IEEE Conference on Network Function Virtualization and Software Defined Networks. Palo Alto, 2017: 167-172.

[16] Zhu Q Y, Başar T. Game-theoretic approach to feedback-driven multi-stage moving target defense[M]. Cham: Springer International Publishing, 2013: 246-263.

[17] Clark A, Sun K ,Bushnell L, et al. Agame-theoretic approach to IP address randomization in decoy-based cyber defense[C]. International Conference on Decision and Game Theory for Security. Cham: Springer, 2015: 3-21.

[18] Yih H, Anup K G. Introducing diversity and uncertainty to create moving attack surfaces for web services[C]. Moving Target Defense. Berlin: Springer, 2011: 131-151.

[19] Hong J B, Kim D S. Assessing the effectiveness of moving target defenses using security models[J]. IEEE Transactions on Dependable and Secure Computing, 2016, 13(2): 163-177.

[20] Forrest S, Somayaji A, Ackley D H. Building diverse

computer systems[C]. Proceedings of the 6th Workshop on Hot Topics in Operating Systems. Cape Cod, 2002: 67-72.

[21] Giuffrida C, Kuijsten A, Tanenbaum A S. Enhanced operating system security through efficient and fine-grained address space randomization[C]. Proceedings of the 21st USENIX Conference on Security Symposium. Bellevue, 2012: 40.

[22] Snow K Z, Monrose F, Davi L, et al. Just-In-time code reuse: On the effectiveness of fine-grained address space layout randomization[C]. IEEE Symposium on Security and Privacy. Berkeley, 2013: 574-588.

[23] Cook K. Kernel address space layout randomization[J]. Linux Security Summit, 2013, 10(9): 27264.

[24] Jang Y, Lee S, Kim T. Breaking kernel addresss pace layout trandomization with intel tsx[C]. Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security. New York: ACM, 2016: 380-392.

[25] Kc G S, Keromytis A D, Prevelakis V. Countering code-injection attacks with instruction-set randomization[C]. Proceedings of the 10th ACM Conference on Computer and Communications Security. Washington DC, 2003: 272-280.

[26] Barrantes E G, Ackley D H, Forrest S, et al. Randomized instruction set emulation to disrupt binary code injection attacks[C]. Proceedings of the 10th ACM Conference on Computer and Communications Security. Washington DC, 2003: 281-289.

[27] Sovarel A N, Evans D, Paul N. Where's the FEEB? The effectiveness of instruction set randomization[C]. USENIX Security Symposium. Piscataway: IEEE, 2005: 1-16.

[28] Portokalidis G, Keromytis A D. Fast and practical instruction-set randomization for commodity systems[C]. Proceedings of the 26th Annual Computer Security Applications Conference. Austin, 2010: 41-48.

[29] Papadogiannakis A, Loutsis L, Papaefstathiou V, et al. ASIST: Architectural support for instruction set randomization[C]. Proceedings of the 2013 ACM SIGSAC Conference on Computer & Communications Security. Berlin, 2013: 981-992.

[30] Bhatkar S, Sekar R. Data space randomization[C]. Detection of Intrusions and Malware, and Vulnerability Assessment. Berlin, 2008: 1-22.

[31] Volckaert S. Randomization-based defenses against data-oriented attacks[C]. Proceedings of the 8th ACM Workshop on Moving Target Defense. Virtual Event, 2021: 1-2.

[32] Rajasekaran P, Crane S, Gens D, et al. CoDaRR: Continuous data space randomization against data-only attacks[C]. Proceedings of the 15th ACM Asia Conference on Computer and Communications Security. Taipei, 2020: 494-505.

[33] Carroll T E, Crouse M, Fulp E W, et al. Analysis of network address shuffling as amoving target defense[C]. IEEE International Conference on Communications. Piscataway: IEEE, 2014: 701-706.

[34] Sharma D P, Kim D S, Yoon S, et al. FRVM: Flexible random virtual IP multiplexing in software-defined networks[C]. The 17th IEEE International Conference on Trust, Security and Privacy In Computing and Communications. New York, 2018: 579-587.

[35] Feng X T, Zheng Z Z, Cansever D, et al. A signaling game model for moving target defense[C]. IEEE INFOCOM 2017—IEEE Conference on Computer Communications. Atlanta, 2017: 1-9.

[36] Fu Z, Papatriantafilou M, Tsigas P. Mitigating distributed denial of service attacks in multiparty applications in the presence of clock drifts[J]. IEEE Transactions on Dependable and Secure Computing, 2012, 9(3): 401-413.

[37] Navas R E, Sandaker H, Cuppens F, et al. IANVS: A moving target defense frame work for a resilient internet of things[C]. IEEE Symposium on Computers and Communications. Piscataway: IEEE, 2020: 1-6.

[38] Danev B, Masti R J, Karame G O, et al. Enabling secure VM-vTPM migration in private clouds[C]. Proceedings of the 27th Annual Computer Security Applications Conference. Orlando, 2011: 187-196.

[39] Rodrigues T G, Suto K, Nishiyama H, et al. Hybrid method for minimizing service delay in edge cloud computing through VM migration and transmission power control[J]. IEEE Transactions on Computers, 2017, 66(5): 810-819.

[40] Duong-Ba T, Tran T, Nguyen T, et al. A dynamic virtual machine placement and migration scheme for data centers[J]. IEEE Transactions on Services Computing, 2021, 14(2): 329-341.

[41] Kampanakis P, Perros H, Beyene T. SDN-based solutions for moving target defense network protection[C]. Proceeding of IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks. Sydney, 2014: 1-6.

[42] Yoon S, Cho J H, Kim D S, et al. Attack graph-based moving target defense in software-defined networks[J]. IEEE Transactions on Network and Service Management, 2020, 17(3): 1653-1668.

[43] Vikram S, Yang C, Gu G. Nomad: Towardsnon-intrusive moving-target defense against web bots[C]. IEEE Conference on Communications and Network Security. Piscataway: IEEE, 2013: 55-63.

[44] Taguinod M, Doup´e A, Zhao A, et al. Toward a moving target defense for web applications[C]. IEEE International Conference on Information Reuse and Integration. Piscataway: IEEE, 2015: 510-517.

[45] Okhravi H, Comella A, Robinson E, et al. Creating a cyber moving target for critical infrastructure applications using platform diversity[J]. International Journal of Critical Infrastructure Protection, 2012, 5(1): 30-39.

[46] Azab M, Hassan R, Eltoweissy M. ChameleonSoft: A moving target defense system[C]. Proceedings of the 7th International Conference on Collaborative Computing: Networking, Applications and Worksharing. Orlando, 2011: 241-250.

[47] Roeder T, Schneider F B. Proactive obfuscation[J]. ACM Transactions on Computer Systems, 2010, 28(2): 1-54.

[48] Jia Q, Wang H, Fleck D, et al. Catch me if you can: A cloud-enabled DDoS defense[C]. The 37th Annual IEEE/IFIP International Conference on Dependable Systems and Networks. Edinburgh, 2014: 264-275.

[49] Bopche G S, Mehtre B M. Graph similarity metrics for assessing temporal changes in attack surface of dynamic networks[J]. Computers & Security, 2017, 64: 16-43.

[50] 雷程, 马多贺, 张红旗, 等. 基于变点检测的网络移动目标防御效能评估方法[J]. 通信学报, 2017, 38(1): 126-140.
(Lei C, Ma D H, Zhang H Q, et al. Performance assessment approach based on change-point detection for network moving target defense[J]. Journal on Communications, 2017, 38(1): 126-140.)

[51] Hong J B, Enoch S Y, Kim D S, et al. Dynamic security metrics for measuring the effectiveness of moving target defense techniques[J]. Comput Secur, 2018, 79: 33-52.

[52] 熊鑫立, 赵光胜, 徐伟光, 等. 基于系统攻击面的动态目标防御有效性评估方法[J]. 清华大学学报: 自然科学版, 2019, 59(4): 276-283.
(Xiong X L, Zhao G S, Xu W G, et al. System attack surface based MTD effectiveness assessment model[J]. Journal of Tsinghua University: Science and Technology, 2019, 59(4): 276-283.)

[53] Xiong X L, Yang L, Zhao G S. Effectiveness evaluation model of moving target defense based on system attack surface[J]. IEEE Access, 2019, 7: 9998-10014.

[54] Sharma D P, Enoch S Y, Cho J H, et al. Dynamic security metrics for software-defined network-based moving target defense[J]. Journal of Network and Computer Applications, 2020, 170: 102805.

[55] Gao C G, Wang Y J, Xiong X L. Comparison of defense effectiveness between moving target defense and cyber deception defense[C]. DSIT 2021: The 4th International Conference on Data Science and Information Technology. Shanghai, 2021: 119-124.

[56] Thompson M, Evans N, Kisekka V. Multiple OS rotational environment an implemented moving target defense[C]. The 7th International Symposium on Resilient Control Systems. Denver, 2014: 1-6.

[57] Chowdhary A, Pisharody S, Huang D J. SDN based scalable MTD solution in cloud network[C]. Proceedings of the 2016 ACM Workshop on Moving Target Defense. Vienna, 2016: 27-36.

[58] 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. Dubai, 2016: 627-630.

[59] 徐潇雨, 胡浩, 张红旗, 等. 基于深度确定性策略梯度的随机路由防御方法[J]. 通信学报, 2021, 42(6): 41-51.
(Xu X Y, Hu H, Zhang H Q, et al. Random routing defense method based on deep deterministic policy gradient[J]. Journal on Communications, 2021, 42(6): 41-51.)

[60] 蒋侣, 张恒巍, 王晋东. 基于多阶段Markov信号博弈的移动目标防御最优决策方法[J]. 电子学报, 2021, 49(3): 527-535.
(Jiang L, Zhang H W, Wang J D. A Markov signaling game-theoretic approach to moving target defense strategy selection[J]. Acta Electronica Sinica, 2021, 49(3): 527-535.)

[61] Feng X T, Zheng Z Z, Cansever D, et al. A signaling game model for moving target defense[C]. IEEE INFOCOM 2017—IEEE Conference on Computer Communications. Atlanta, 2017: 1-9.

[62] Lei C, Zhang H Q, Wan L M, et al. Incomplete information Markov game theoretic approach to strategy generation for moving target defense[J]. Computer Communications, 2018, 116: 184-199.

[63] Zhou Y Y, Cheng G, Jiang S Q, et al. A cost-effective shuffling method against DDoS attacks using moving target defense[C]. Proceedings of the 6th ACM Workshop on Moving Target Defense. London, 2019: 57-66.

[64] Sengupta S, Kambhampati S. Multi-agent reinforcement learning in Bayesian stackelberg Markov games for adaptive moving target defense[J/OL]. 2020, arXiv: 2007.10457.

[65] 陈子涵, 程光. 基于Stackelberg-Markov非对等三方博弈模型的移动目标防御技术[J]. 计算机学报, 2020, 43(3): 512-525.
(Chen Z H, Cheng G. Moving target defense technology using stackelberg Markov asymmetrical trilateral game model[J]. Chinese Journal of Computers, 2020, 43(3): 512-525.)

[66] Tan J L, Zhang H W, Zhang H Q, et al. Optimal temporospatial strategy selection approach to moving target defense: A flipIt differential game model[J]. Computers & Security, 2021, 108: 102342.

[67] 熊鑫立, 杨林, 李克超. 基于马尔可夫决策过程的动态目标防御策略优化方法[J]. 武汉大学学报: 理学版, 2020, 66(2): 141-148.
(Xiong X L, Yang L, Li K C. A strategy optimization model of moving target defense based on Markov[J]. Journal of Wuhan University: Natural Science Edition, 2020, 66(2): 141-148.)

[68] Eghtesad T, Vorobeychik Y, Laszka A. Adversarial deep reinforcement learning based adaptive moving target defense[M]. Lecture Notes in Computer Science. Cham: Springer International Publishing, 2020: 58-79.

[69] Sengupta S, Kambhampati S. Multi-agent reinforcement learning in Bayesian stackelberg Markov games for

adaptive moving target defense[J/OL]. 2020, arXiv: 2007.10457.

[70] Gao C G, Wang Y J. Reinforcement learning based self-adaptive moving target defense against DDoS attacks[J]. Journal of Physics: Conference Series, 2021, 1812(1): 012039.

[71] Nizzi F, Pecorella T, Esposito F, et al. IoT security via address shuffling: The easy way[J]. IEEE Internet of Things Journal, 2019, 6(2): 3764-3774.

[72] Ge M M, Cho J H, Kim D S, et al. Proactive defense for Internet-of-things: Integrating moving target defense with cyberdeception[J/OL]. 2020, arXiv: 2005.04220.

[73] Peng W, Li F, Huang C T, et al. A moving-target defense strategy for cloud-based services with heterogeneous and dynamic attack surfaces[C]. 2014 IEEE International Conference on Communications. Sydney, 2014: 804-809.

[74] Azab M, Eltoweissy M. MIGRATE: Towards a lightweight moving-target defense against cloud side-channels[C]. 2016 IEEE Security and Privacy Workshops. San Jose, 2016: 96-103.

[75] Sengupta S, Chowdhary A, Huang D, et al. Moving target defense for the placement of intrusion detection systems in the cloud[C]. International Conference on Decision and Game Theory for Security. Cham: Springer, 2018: 326-345.

[76] Jin H, Li Z, Zou D Q, et al. DSEOM: A framework for dynamic security evaluation and optimization of MTD in container-based cloud[J]. IEEE Transactions on Dependable and Secure Computing, 2019, 18(3): 1125-1136.

[77] 王琦, 郤伟, 汤奕, 等. 面向电力信息物理系统的虚假数据注入攻击研究综述[J]. 自动化学报, 2019, 45(1): 72-83.
(Wang Q, Tai W, Tang Y, et al. A review on false data injection attack toward cyber-physical power system[J]. Acta Automatica Sinica, 2019, 45(1): 72-83.)

[78] Lakshminarayana S, Yau D K Y. Cost-benefit analysis of moving-target defense in power grids[J]. IEEE Transactions on Power Systems, 2020, 36(2): 1152-1163.

[79] Higgins M, Teng F, Parisini T. Stealthy MTD against unsupervised learning-based blind FDI attacks in power systems[J]. IEEE Transactions on Information Forensics and Security, 2020, 16: 1275-1287.

[80] 张镇勇. 智能电网中面向错误数据注入攻击的移动目标防御研究[D]. 杭州: 浙江大学, 2020.
(Zhang Z Y. Moving target defense against false data injection attack in smart grid[D]. Hangzhou: Zhejiang University, 2020.)

[81] Lakshminarayana S, Belmega E V, Poor H V. Moving-target defense against cyber-physical attacks in power grids via game theory[J]. IEEE Transactions on Smart Grid, 2021, 12(6): 5244-5257.

[82] Liu B, Wu H Y. Optimal planning and operation of hidden moving target defense for maximal detection effectiveness[J]. IEEE Transactions on Smart Grid, 2021, 12(5): 4447-4459.

[83] Roy A, Chhabra A, Kamhoua C A, et al. A moving target defense against adversarial machine learning[C]. Proceedings of the 4th ACM/IEEE Symposium on Edge Computing. Arlington, 2019: 383-388.

[84] Wang W W, Xiong X L, Wang S H, et al. MTDNNF: Building the security framework for deep neural network by moving target defense[C]. ACAI 2020: 2020 3rd International Conference on Algorithms, Computing and Artificial Intelligence. Sanya, 2020: 1.

[85] Amich A, Eshete B. Morphence: Moving target defense against adversarial examples[C]. Annual Computer Security Applications Conference. Virtual Event, 2021: 61-75.

[86] Magdy Y, Kashkoush M S, Azab M, et al. Anonymous blockchain based routing for moving-target defense across federated clouds[C]. 2020 IEEE 21st International Conference on High Performance Switching and Routing. Newark, 2020: 1-7.

[87] He G F, Si Y R, Xiao X C, et al. Preventing IoT DDoS attacks using blockchain and IP address obfuscation[C]. 2021 13th International Conference on Wireless Communications and Signal Processing. Changsha, 2021: 1-5.

[88] Woo S, Moon D, Youn T Y, et al. CAN ID shuffling technique (CIST): Moving target defense strategy for protecting In-vehicle CAN[J]. IEEE Access, 2019, 7: 15521-15536.

[89] Lee S, Kim H K, Kim K. Ransomware protection using the moving target defense perspective[J]. Computers & Electrical Engineering, 2019, 78: 288-299.

作者简介

姚倩 (1999−), 女, 硕士生, 从事移动目标防御、智能化网络安全测试等研究, E-mail: yaoqian21@nudt.edu.cn;

熊鑫立 (1991−), 男, 讲师, 博士, 从事移动目标防御、大规模网络对抗技术等研究, E-mail: xiongxinli_@nudt.edu.cn;

王永杰 (1974−), 男, 教授, 博士, 从事网络控制与利用、网络安全建模与仿真、移动目标防御等研究, E-mail: wangyongjie17@nudt.edu.cn;

侯冬冬 (1992−), 女, 讲师, 博士, 从事机器学习、数据挖掘、多源数据融合、网络空间安全等研究, E-mail: houdongdong22@nudt.edu.cn.