基于网络空间欺骗的移动目标防御技术研究

张雅勤 [1,3], 马多贺 [1,3], Xiaoyan Sun [2], 周 川 [1,3], 刘 峰 [1,3]

[1] 中国科学院信息工程研究所信息安全国家重点实验室 北京 中国 100093

[2] Department of Computer Science, California State University, Sacramento, USA 95819

[3] 中国科学院大学网络空间安全学院 北京 中国 100093

摘要 移动目标防御(Moving Target Defense, MTD)是改变当前网络空间“易攻难守”的攻防不对称局面的革命性技术之一。MTD 的基本思想是通过持续不断地转换攻击面, 增加攻击者攻击的困难度和复杂度。如何选取转换属性, 提高属性攻击面转换空间是 MTD 领域研究的重点问题。多样化、冗余和欺骗是当前属性攻击面转换空间构造的主要方法。其中, 多样化和冗余策略在构建攻击面转换空间时, 存在构建成本高以及系统兼容性等问题, 使得传统的移动目标防御无论在理论研究, 还是在实际应用中都遇到了很大瓶颈。而欺骗策略则为解决这一困难问题提供了契机。欺骗策略由于其虚虚实实的变化, 蜜罐、蜜饵、面包屑等多样化的欺骗方式, 以及构建成本低、构造欺骗属性容易等特性, 被提出用于扩大攻击面转换空间, 成为 MTD 研究的重要技术手段和工具。首先, 比较了基于网络空间欺骗的 MTD 与经典 MTD(基于多样化和冗余的 MTD) 的差异, 明确了网络空间欺骗在移动目标防御中发挥的重要价值; 然后, 基于 MTD 攻击面理论, 提出了欺骗攻击面的概念, 并基于此概念对欺骗移动目标防御进行了形式化定义; 接着, 根据网络空间欺骗机制的作用范围和需应对的攻击威胁, 从网络层、系统层、应用层和数据层对基于欺骗的 MTD 技术及其应用进行了探索与分类, 并从理论和实验两个维度总结基于欺骗的 MTD 有效性的评估方法; 最后, 归纳了研究面临的主要问题与挑战, 并讨论了未来可能的研究方向。

关键词 移动目标防御; 网络空间欺骗; 网络空间安全; 评估方法

中图法分类号 TP393 **DOI 号** 10.19363/J.cnki.cn10-1380/tn.2023.06.04

A Study on Cyber Deception-Based Moving Target Defense

ZHANG Yaqin[1,3], MA Duohe[1,3], SUN Xiaoyan[2], ZHOU Chuan[1,3], LIU Feng[1,3]

[1] State Key Laboratory Of Information Security, Institute of Information Engineering, CAS, Beijing 100093, China

[2] Department of Computer Science, California State University, Sacramento 95819, USA

[2] School of Cyber Security, University of Chinese Academy of Sciences, Beijing 100093, China

Abstract Moving Target Defense(MTD) is one of the game-changing revolutionary concepts that surpasses traditional approaches by wresting the asymmetric advantages of the attackers over defenders. The basic idea of MTD is to continuously change the attack surface, thereby increasing the difficulty and complexity of attackers. Choosing the attributes to switch and expanding the switching space of attribute attack surface are critical problems in MTD research. Currently, diversification, redundancy and deception are three main strategies for constructing the switching space. However, the high cost and system incompatibility issues of the first two strategies, together with the limited attack surface switching space, make the theoretical research and practical application of traditional MTD remain stagnant. Cyber deception strategy provides an opportunity for this challenging problem. It offers diversified deceptive methods, such as honeypots, honey baits, and breadcrumbs, and has the characters of low cost and easy construction of deceptive properties. Therefore, cyber deception strategy now is used to expand the attack surface switching space, and becomes one of the most important approaches and tools for MTD study. In this paper, we first compare the differences between traditional MTD and cyber deception-based MTD, and identify the important value of cyber deception in MTD. Then based on attack surface theory given in MTD, we propose the concept of deception attack surface, and present the formalized definition of cyber deception based moving target defense based on this concept. Furthermore, according to the scope of the deception mechanism and the cyber threats to be dealt with, we perform a multi-dimension classification towards existing works in cyber deception-based MTD from four perspectives: network, system, application and data. Beyond that we present the evaluation methods for deception-based MTD validity from the theoretical and experimental dimensions. Finally, we summarize the limitations and challenges of existing solutions, and discuss potential future research directions.

Key words moving target defense; cyber deception; cybersecurity; evaluation

---

通讯作者: 马多贺, 博士, 副研究员, CCF 高级会员, Email: maduohe@iie.ac.cn。

本课题得到国家重点研发计划(No. 2018YFC0806900), 国家自然科学基金(No. 61671448、No. 61902397)和中国科学院信息工程研究所“青年之星”项目(No. Y7Z0201105)的资助。

收稿日期: 2020-10-25; 修改日期: 2021-04-08; 定稿日期: 2023-02-23

1 引言

随着信息化技术的发展, 社会信息化进程不断加速, 计算机网络逐渐渗透到经济、社会、政治、生活的各个方面, 网络空间亦成为涵盖政府、商业、金融、通信、军事等重要领域的国家战略资源, 网络空间安全受到世界各国高度重视。

然而, 近十年来频繁曝出的重大安全事件表明网络安全始终面临严峻挑战。2010 年伊朗核电站遭到 Stuxnet 震网蠕虫攻击事件曝光, 2014 年互联网曝出基于 OpenSSL 协议的 Heart Bleed 漏洞, 2017 年国内众多高校受 Wannacry 勒索病毒影响, 2018 年首次披露针对乌克兰 IoT 设备的恶意代码攻击事件, 2019 年印度最大的核电站遭到 APT 攻击, 等等。当前, 网络攻击正从低级别的攻击向目标更明确、危害更严重的高级别攻击转变, 金融、交通、能源等关键基础设施网络逐渐成为重点攻击目标, 网络攻击的破坏性急剧增加, 防御成本显著提高。网络空间安全已成为事关国家安全、经济发展和社会稳定的战略性课题。将网络空间安全提升至国家安全, 构建网络空间安全体系, 增强网络空间安全防御能力成为世界各国努力的方向。

传统的网络防御思想是在现有的网络体系架构上, 通过修补漏洞、构建防火墙、入侵检测、访问控制、数据加密等多层次的网络防御体系提升网络安全。然而, 不断增多的重大网络安全事件表明, 现有的网络安全防御体系难以有效应对不断发展的网络攻击手段, 网络空间正面临“易攻难守”的不对称局面。造成这一局面的原因在于传统网络系统的确定性、静态性和相似性特点: 确定性, 使攻击者具备时间优势。攻击者可以长时间对目标进行扫描和探测, 分析目标系统的脆弱性; 静态性, 使攻击者具备空间优势。攻击者只需掌握少量可利用的漏洞信息, 即可通过一定途径或方法发动攻击, 而防御者则需要考虑所有可能出现的脆弱点和攻击途径; 相似性, 攻击者一旦成功实施一次攻击, 就可以较低的成本将攻击扩大到更大范围的类似网络系统, 攻击成本显著降低。日益复杂的攻击手段和层出不穷的漏洞使传统的静态防御方法愈显被动。为改变网络空间面临的“易攻难守”的不对称局面, 提高网络系统应对攻击威胁的能力, 发展动态的、主动的网络防御技术成为网安全领域的重要研究方向。

移动目标防御(Moving Target Defense, MTD)是网络空间中“改变游戏规则”的革命性技术之一: 构建、评价和部署机制及策略是多样的、不断变化的。这种不断变化的思路可以增加攻击者的攻击难度及代价, 有效限制脆弱性暴露及被攻击的机会, 提高系统的弹性[1]。因此, 动态的变换目标系统攻击面, 使其成为“移动目标”, 被认为能有效防止进攻方收集网络的安全信息, 从而大大提高网络防御的效能[2] 。

移动目标防御通过不断改变目标系统的属性来动态转换其攻击面, 因此如何构建充足的属性转换空间是 MTD 研究的核心问题之一。多样化、冗余和欺骗是当前属性转换空间构造的主要策略。其中, 多样化策略旨在为某个属性创建多个可替换的属性值, 但构建功能等价的数据格式有很高的困难性, 且会导致系统的不兼容问题; 冗余策略采用多个功能相同的副本同时在线工作, 且不要求属性值有差异, 使得目标系统缺少差异性, 导致攻击者会继续对存在漏洞的系统进行重复的攻击。多样化和冗余策略的缺陷使传统的移动目标防御无论在理论研究, 还是在实际应用中都遇到了很大瓶颈。欺骗策略由于其多样化的欺骗方式, 如蜜罐、蜜饵、蜜标、面包屑等, 以及构建成本低、构造欺骗属性容易等特性, 为扩大攻击面转换空间提供了新的方向, 成为 MTD 研究的重要技术手段和工具。网络空间欺骗主要是通过使用骗局或假动作掩盖真实的目标系统或资源, 阻挠或推翻攻击者的认知过程, 延迟或阻断攻击者的活动, 使用虚假的响应、有意的混淆以及假动作、误导等伪造信息达到“欺骗”的目的[3]。网络空间欺骗通过在目标系统的真实属性内填充虚假的属性值, 或创建提供虚假功能的属性, 掩饰防御目标的真实攻击面, 改变攻击者对目标系统的认知。

当前移动目标防御研究得到了大量研究者的关注, 众多针对性的移动目标防御技术被提出, 大量文献也从理论和实验角度验证了移动目标防御的有效性, 但是构造攻击面转换空间的高成本、高代价, 为其在网络空间的进一步研究、应用提供了很大的障碍。因此关注基于网络空间欺骗的 MTD 研究, 探索欺骗在 MTD 中的应用, 以应对愈加智能化的攻击挑战至关重要。本文首先比较了基于网络空间欺骗的 MTD 与经典 MTD 的差异, 明确了网络空间欺骗在移动目标防御中发挥的重要价值, 然后根据已有研究从多维度对基于欺骗的MTD技术进行了探索与分类, 并总结了欺骗 MTD 的有效性评估方法, 最后归纳了研究面临的主要问题与挑战, 并讨论了未来可能的研究方向。

2 相关研究

2.1 网络空间欺骗

早在 1989 年, Cliff Stoll 就在《The Cuckoo’s Egg》

一书中提出将欺骗用于增加系统的安全性[4]。作者提出了构建一个虚构的系统环境的方法，比如通过一个填充了大量虚假文件的账户故意吸引攻击者的注意力，延迟攻击者的攻击，同时追踪并分析攻击者的来源。通过利用虚构的环境设计吸引并捕获攻击者，逐渐发展成为广受欢迎的蜜罐。后续相继提出了蜜标、蜜饵、面包屑、蜜词本、无底洞文件等欺骗技术，进一步保护计算机系统和网络。

欺骗防御的主要流程分为三个阶段(如图 1)：欺骗设计、欺骗实现与部署、欺骗效果评估。在欺骗设计阶段，基于对敌人的意图、利益和能力的初步了解，防御者首先会明确可以按合理预期实现的欺骗目标。欺骗设计应包括如何与攻击者交互，如何设计导致攻击者认知偏差的欺骗信息，这是欺骗防御成功的关键。在欺骗实现与部署阶段，根据欺骗计划，欺骗组件可以包含设备(主机或服务器)、设备上的信息和设备之间的通信。因为欺骗防御注重于改变攻击者对目标系统的认知，所以在欺骗部署后，必须实时追踪攻击者的行为轨迹，观察攻击者的反应。

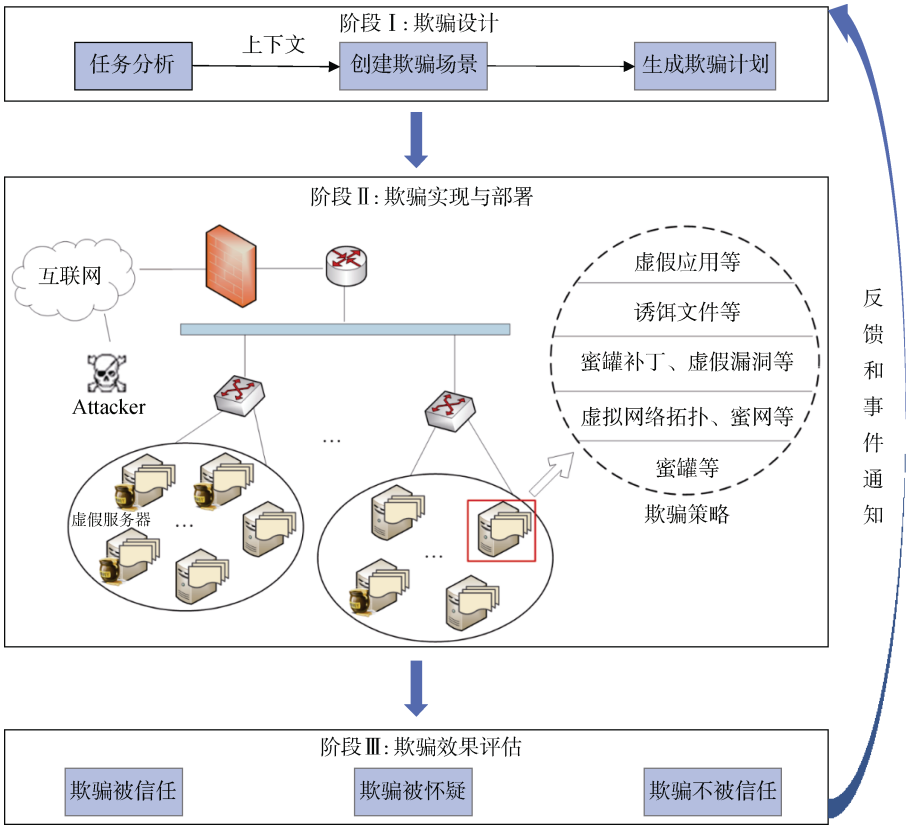

图 1　欺骗防御主要流程

Figure 1　Primary Phases of Deception Defense

网络空间欺骗是实现主动防御的重要方式，也是一种有效的、互补的防御技术。网络空间欺骗故意将错误信息或误导信息引入网络空间，以此欺骗攻击者，增加攻击的复杂度。欺骗可以弥补传统检测、防御策略面临的攻防不对称挑战，改变传统防御中防御者在面临攻击者时的被动劣势，从而使网络攻防对抗处于平衡状态。

2.2　MTD 属性攻击面转换空间的实现机制

传统的网络防御方法通过修补系统漏洞，部署网络安全防御设备等措施减小目标系统的攻击面，提高网络的安全性。移动目标防御通过不断地转换攻击面，使攻击者花费更多的时间和成本定位或重新定位目标系统的位置和漏洞，从而限制网络脆弱性暴露和被攻击的机会。MTD 动态、主动地改变目标系统属性的特性引起了研究人员的关注。如何选取攻击面中需要转换的属性，提高属性攻击面转换空间是MTD 领域研究的重点问题。多样化(Diversity)、冗余(Redundancy)和欺骗(Deception)是当前属性攻击面转换空间构造的主流方法。

多样化是指通过为目标系统的某个属性创建多个可替换的属性值。随机化方法主要是为目标系统的某个属性创建一个可替换的属性值，是多样化方法的特例。基于数据的多样化[5-6]；基于软件的多态化[7]，地址空间布局随机化[8]，指令集随机化[9]，代码

随机化[10-11]; 基于网络的网络地址随机化[12-13], 端口信息随机跳变[14]; 基于平台的动态迁移[15], 虚拟化技术[16]等。复杂的网络空间环境为攻击者的探测、攻击增加了难度, 但是构建多种功能等价的属性的困难性和属性样式的有限性, 使属性的攻击面转换空间受限, 且多样化策略对系统和程序代码的修改也会造成很大的开销。

冗余是指采用多个功能相同的副本同时在线工作, 且不要求属性值有差异。Kirrmann 等[17]提出将冗余应用于任意层的通信栈(物理层、链路层、网络层), 如使用路径冗余[18]提高数据传输的安全性, 使用软件冗余[19], 数据冗余[20], 服务器冗余[21]等减弱攻击的范围。但是由于目标系统缺少差异性, 攻击者仍然可以对存在漏洞的系统进行重复的攻击。

欺骗是指在真实的属性值之外进行扩充, 扩充部分是虚假的。Bell and Whaley(1991)[22]提出了经典的欺骗方法分类, 为欺骗的研究开展提供了很好的支撑。按照计算机体系及网络分层模型, 网络空间欺骗机制研究可以分为软件、数据、网络、应用四个层次。基于数据的虚假文档[1]、虚假密码 honeywords[23], 基于网络的虚拟网络拓扑[24]、端口返回信息混淆[25], 基于 web 应用的 phoneytoken[26]、虚假链接[27]等欺骗技术均为网络空间提供了很好的防御策略, 然而当前基于欺骗的研究是粗粒度的, 无法抵抗多样化、智能化的攻击手段。进一步地, 为了应对内部入侵者的威胁, 在移动目标防御中引入欺骗技术, 改变基于属性的访问控制机制中的属性规则[28]方法被提出; 此外, 为了主动的抵御网络攻击, 提出了动态的主机突变架构, 采用系统指纹欺骗的方式, 增加攻击者探测目标系统指纹的成本[29]。作为扩大属性攻击面转换空间的重要手段, 将欺骗引入移动目标防御, 为应对层出不穷的网络攻击手段提供了重要的研究方向。

网络空间欺骗进一步提高了 MTD 系统的安全性。如表 1 所示, 比较了 MTD 与网络空间欺骗的异同点: 一方面, 移动目标防御与网络空间欺骗是互为补充的主动防御方法; 另一方面, 移动目标防御通过不断改变系统的配置, 增加系统的复杂性, 多样性和随机性, 从而扰乱了敌手的勘测和攻击计划。而网络空间欺骗主要是通过提供看似真实但虚假的信息, 误导攻击者的行动, 从而使其攻击错误的目标对象, 分散其在真实目标系统的注意力, 增加 MTD 系统的安全性。

当前众多经典的欺骗 MTD 技术被提出:

嵌入网页欺骗组件的 web MTD[30-32]。通过在网页中加入欺骗元素, 当恶意用户爬取、执行 XSS、钓鱼等攻击时便会中计。如 honey links[27], honey files[30], decoy forms[31], 以及数据库中的 honey data[32]等欺骗方法的提出均为诱导攻击者进入陷阱, 增加攻击者获取信息的难度。

表 1 移动目标防御与网络空间欺骗的比较

Table 1 Comparison between MTD and cyber deception

		MTD	网络空间欺骗
相同点		主动防御, 保护目标系统	
差异点	技术方法	改变系统的配置, 增加系统的复杂性和多样性, 使系统的变化速率要快于攻击者的攻击勘测速率。	不专注于改变系统的配置, 而是通过主动地泄露部分信息, 分散敌手注意力, 从而隐藏真实的目标系统。
	信息泄露	否, 主要是阻止攻击者收集信息	是, 泄露非必要的部分真实信息或精心设计的虚假信息
	成本	高, 对系统有较高负载	低, 部署设置更简单, 降低系统负载
	对象	理解系统	理解敌手
关系		MTD 与网络空间欺骗是互补的防御技术, 且网络空间欺骗能够进一步提高 MTD 系统的安全性。	

构造“白洞”欺骗的网络 MTD[33-34]。针对网络扫描攻击, 采用返回信息混淆的方式, 欺骗应答目标系统的所有的端口都是开放的, 使攻击者难以获取有用的信息, 实现移动目标防御的目的。

伪造诱饵文件欺骗的数据 MTD[35]。通过部署虚假文件、数据库表项等欺骗攻击者, 诱导网络入侵者相信目标系统存在有价值的资源数据, 使其相信这些有价值而实际上是伪造的资源, 增加其入侵难度。数据作为网络系统中最有价值的资产, 也是敌手首要的攻击目标。基于欺骗的数据 MTD 可以进一步缓解数据泄露问题。

欺骗即服务(Deception as a Service)[36-37]。通过按需构建多样化的欺骗方式, 提供一站式的欺骗解决方案。由于目标系统多变的欺骗方式, 攻击者无法攻击访问真实的服务器。研究人员基于这一特性设置的欺骗代理服务器, 既提供了针对多种网络威胁的综合解决方案, 也可以在客户端提供良好的用户体验, 可以广泛应用在具有特殊安全和保密需求的场合中。

在过去的二十年中, 人们在网络空间中探索了各种形式的欺骗策略并提出了多种技术解决方案。然而, 对欺骗技术的理论基础及其在网络空间安全中的应用研究仍然不足。研究文献中也很少涉及对欺骗技术的建模, 部署, 更新和评估等的总结, 难以

将欺骗技术与其他方法进行比较。因此探讨并总结基于欺骗的技术, 从不同维度对网络空间欺骗进行探索和分类研究, 归纳并分析网络空间欺骗的相关工作, 理解网络空间欺骗在 MTD 系统的价值, 对后续的研究具有重要意义。

文章后续分别从基于网络空间欺骗的机理建模(第 3 章节), 机制研究分析(第 4 章节), 以及安全度量评估(第 5 章节), 三个方面进行了深度剖析, 从多维度对网络空间欺骗进行了更细致的分类与划分, 并探索了网络空间欺骗技术的引入对MTD及网络空间安全性的影响。

3 基于网络空间欺骗的 MTD 机理建模

移动目标防御可以利用攻击面(Attack Surface)理论进行解释。攻击面的概念最早由 Manadhata 等人[38-39]提出, 并将攻击面作为度量系统安全的指标。系统的攻击面是可被攻击者利用并发动攻击的系统脆弱性资源的集合, 是系统暴露给攻击者进入系统并实施攻击的各种途径。目标系统的攻击面越大, 系统的安全性越低。

攻击者在发动攻击前需要对目标系统的资源进行探测和勘察, 因此引入探测面(Exploration Surface)的概念用于表示攻击者所需要探测和侦查的空间。以 IP 地址为例, 解释探测空间的概念。例如, 一台主机运行在某个典型的 C 类子网中(假设 IP 地址为 192.168.0.X), 若该主机的 IP 地址在地址空间中不断变化, 攻击者不能确定某个时刻该主机的 IP 地址, 那么攻击者的探测空间即为集合{192.168.0.1, 192.168.0.2, …., 192.168.0.254}, 探测空间大小为 254。若该主机的 IP 地址固定, 则攻击者的探测空间大小将为 1。目标系统的探测空间越大, 则攻击者发现并定位攻击目标的难度和成本越大, 相应地, 网络安全性越高。

图 2 对比了传统网络防御、经典移动目标防御和基于网络空间欺骗的移动目标防御: 传统网络防御旨在, 减小攻击面; 经典 MTD 专注于转换攻击面; 而基于欺骗的MTD则更注重创建欺骗攻击面以扩大攻击面转换空间。

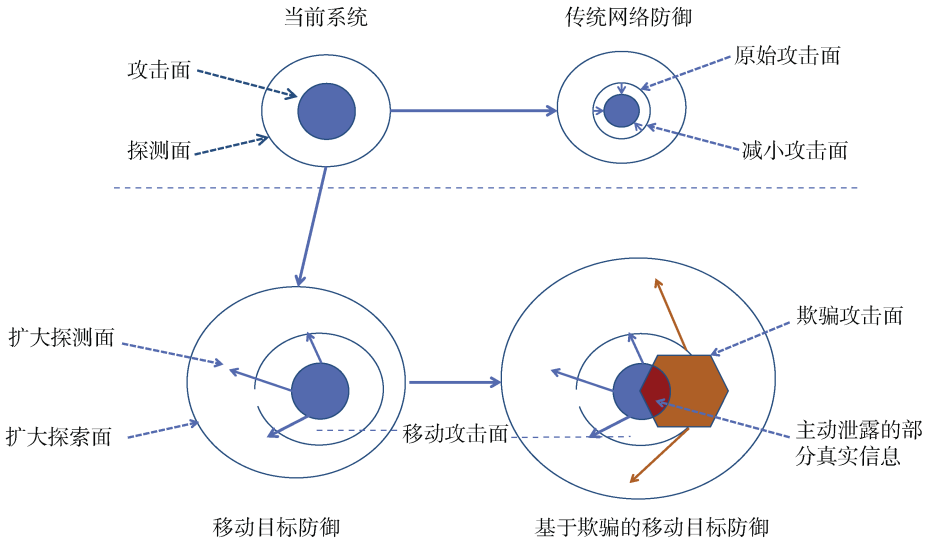

图 2 欺骗移动目标防御与经典移动目标防御、传统网络防御的对比

Figure 2 Comparison among Traditional Network Defense, MTD and Deception-based MTD

3.1 基于攻击面的欺骗 MTD 模型

基于攻击面理论, 本文提出了欺骗攻击面的思想。网络空间欺骗没有修改系统的真实攻击面, 而是通过创建虚假的攻击面, 改变了攻击者对系统攻击面的认知。将引入欺骗元素后攻击者探测并感知到的攻击面定义为**欺骗攻击面**(Deception Surface), 欺骗攻击面的设计越巧妙, 越可以吸引攻击者的注意力, 从而隐藏真实的目标系统。

图 3 描述了基于网络空间欺骗的MTD的基本思想。欺骗可以创建虚假的攻击面, 与多样化、冗余方法结合, 将创建更加丰富的攻击面变化。如图 3 中表示的冗余方法中的副本 1 与副本 2 所示, 冗余是采用多个功能相同的副本同时在线工作, 不要求副本之间的实现有差异; 多样化是创建多个可替换的版本, 采用不同的方法实现的版本交替工作; 欺骗是通过主动泄露部分真实的信息引诱攻击者, 并部署欺骗环境诱使攻击者攻击虚假的版本。当欺骗与冗余方法结合时, 亦是多个副本同时在线工作, 但是其中引入了欺骗副本, 任何尝试连接欺骗副本的用户都被认为是异常用户或攻击者; 当欺骗与多样化方法

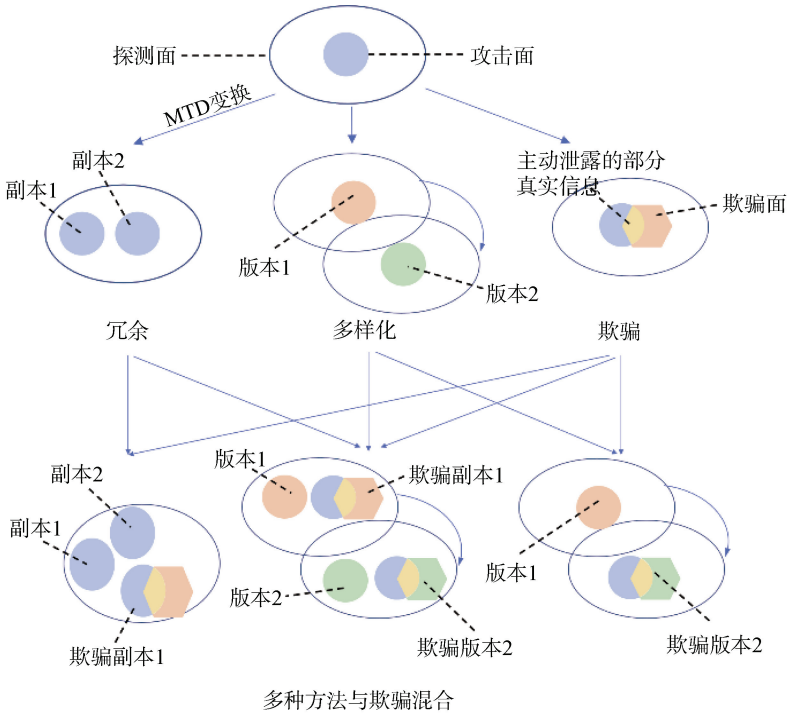

图 3　基于网络空间欺骗的 MTD

Figure 3　Basic Idea of Cyber Deception-Based MTD

结合时, 则欺骗版本与其它非欺骗版本交替工作; 当三种方法结合时, 则多个不同的版本同时在线工作, 包括多样化的非欺骗版本和欺骗版本。

Albanese 等人[40]以操作系统这一属性为例, 基于图论建立了操作系统属性的欺骗攻击面, 以此类比, 亦可将此图论思想推而广之, 拓展到网络空间, 利用有向图表示攻击面的变换过程。基本思想如下:

假定攻击者对系统的认知为 A, 防御者对系统的认知为 D, 则系统攻击面可定义为没有采用欺骗策略时暴露给攻击者的 D 的子集。欺骗的目的是使攻击者对系统攻击面的认知不同于 D。

假定系统可以用一个集合表示为 $S=\{S_1,S_2,S_3,\cdots,S_n\}$, 其中 $S_{n(n=1,2,3\cdots)}$ 表示系统设备, 如主机, 防火墙等。φ 表示 S 中主机所能提供的服务的集合。防御者与攻击者对系统的认知可以用视图表示, 定义如下:

定义 1. 系统视图: 给定系统 S, S 的视图可以定义为 $V=(S_0,C,v)$, 其中 $S_0\subseteq S$ 表示可观察到的设备的集合, $C=S_0\times S_0$ 表示 S_0 中元素之间的连通性, $v:S_0\to 2^{\varphi}$ 表示 S_0 中每个主机到其所能提供的服务集合的映射函数。

定义 2. 视图转换图(View Manipulation Graph): 给定系统 S, 系统 S 的视图集合 v, 转换函数族 Π, 则系统 S 的视图转换图可以表示为一个有向图 $G=(v',\varepsilon,\ell)$, 其中:

(1) $v'\subseteq v$ 表示 S 的视图的集合

(2) $\varepsilon\subseteq v\times v$ 表示边的集合

(3) $\ell:\varepsilon\to\prod$ 表示与每条边 $(v',v'')\in\varepsilon$ 相关的转换函数。如转换函数 $\pi\in\prod$ 作用于视图 v', 从而得到新的视图 v'', 即 $v''=\pi(v')$。

如图 4 所示, 视图转换图表示了目标系统从真实攻击面向欺骗攻击面进行变换的过程。图中每个顶点表示系统 S 的某个视图, 每条有向边表示视图的转换操作。从图中顶点 V 开始, 可通过修改操作系统的指纹, 转换成新的视图 V_1, 进而又对邮件服务器部署其它欺骗技术, 得到新的视图 V_2。

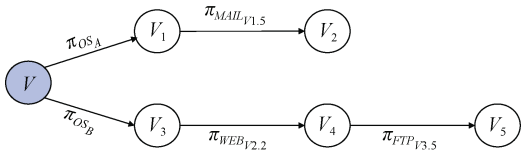

图 4　移动目标防御攻击图

Figure 4　The Attack Graph of Moving Target Defense

3.2　基于攻击图的欺骗 MTD 模型

攻击图是同时考虑目标系统的脆弱性、攻击目标和节点连接性, 描述导致系统状态转移的复杂攻击序列的一种方法。图 5 和图 6 对比了基于网络空

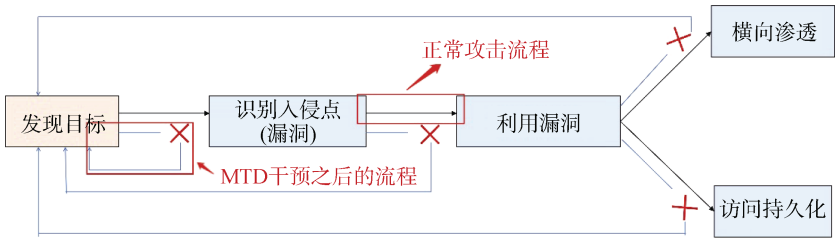

图 5　基于欺骗的移动目标防御攻击图

Figure 5　The Attack Surface of Deception-Based Moving Target Defense

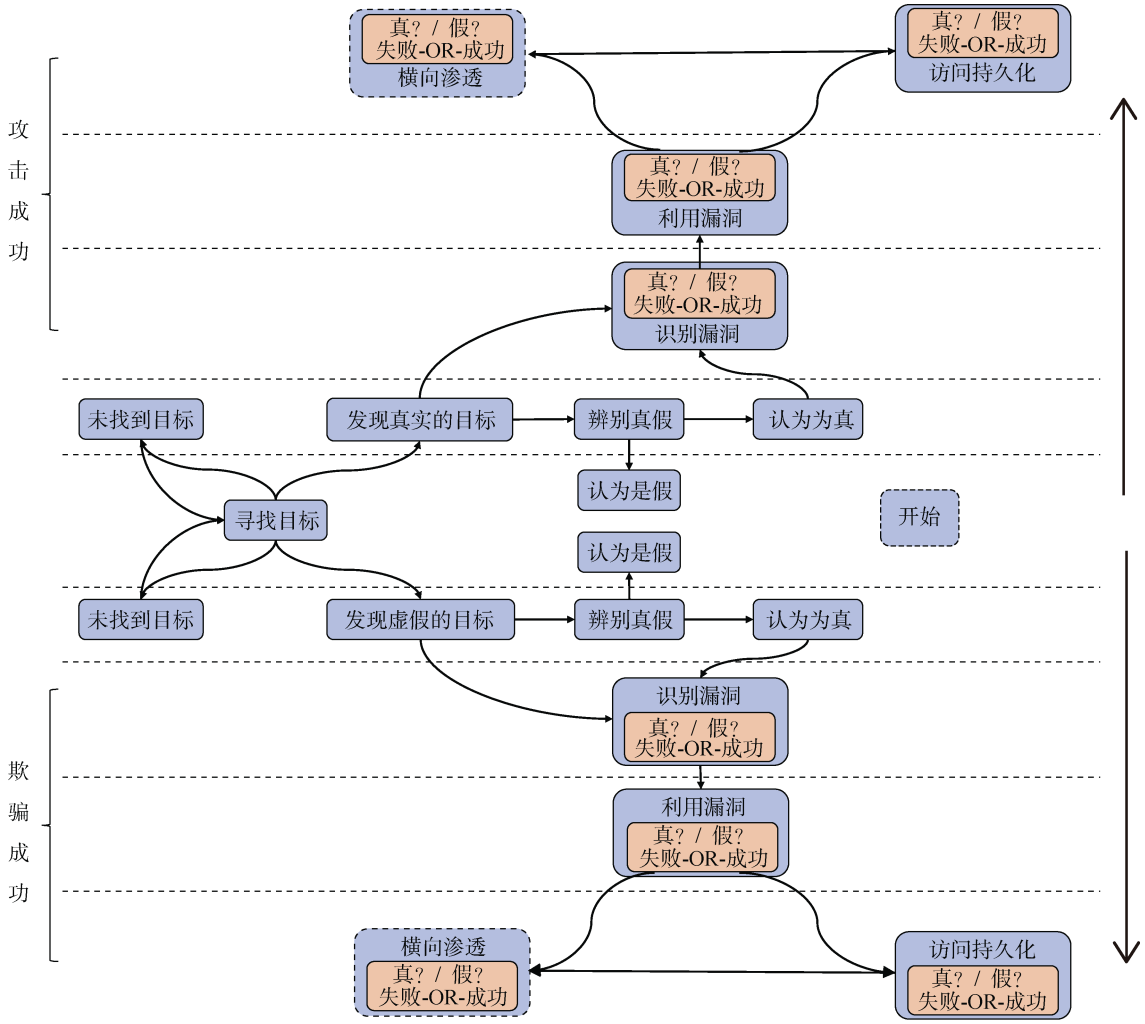

图 6　视图转换图实例

Figure 6　Example of View Manipulation Graph

间欺骗的 MTD 与非欺骗的 MTD 攻击图。攻击的主要流程可以分为发现目标(勘测)、识别入侵点(漏洞)、利用漏洞、横向渗透和访问持久化。MTD 方法可以在一次攻击完成前的任何攻击阶段, 使攻击无效。在攻击者进行不断地扫描、勘测, 发现目标时, 可能会由于目标系统 IP 地址跳变或指纹跳变, 增加其探测目标的难度。进一步地, 当攻击者经过勘测, 发现目标后, 在要进一步识别目标系统漏洞时, 也可能由于目标系统通过 IP 地址随机化或端口跳变操作, 需要重新探测目标。此外, 当攻击者识别漏洞成功, 准备利用漏洞发起攻击时, 目标系统可能会通过平台动态迁移方法, 对系统攻击面进行了动态转移, 使攻击者利用漏洞失败, 无法进入攻击的下一阶段。因而, MTD 对攻击者主要有两个实质性的影响: 一是增加攻击者“发现目标”阶段, 即探测阶段的成本; 二是在攻击流程内, 由于攻击面的动态变化, 使攻击者从其他状态返回到“发现目标”这一初始阶段, 重新探测原始目标的位置。在某种程度上, “发现目标”

是 MTD 系统中攻击者被击败的主要阶段。而引入欺骗后, 更是加大了攻击者“发现目标”的难度。

4 基于网络空间欺骗的机制研究

根据网络空间欺骗机制的作用范围可以分为网络层, 系统层, 应用层和数据层。网络层涵盖可通过网络访问且不受任何特定主机配置约束的欺骗技术; 系统层涵盖基于主机的欺骗技术; 应用层涉及特定类的应用程序欺骗技术, 如 web 应用程序或数据库等; 数据层涵盖了利用用户特定数据(如虚假账户或虚假文档)的欺骗技术。本文基于需应对的攻击威胁, 对各层欺骗机制进行了进一步分类。

4.1 网络层欺骗

网络层欺骗在MTD中主要是通过部署诱饵节点, 构建虚假网络拓扑, 或利用欺骗响应, 诱导攻击者, 以及指纹欺骗。网络层欺骗主要是应对探测阶段的攻击。

(1) IP 地址和端口跳变

在 IP 地址跳变方面, 有研究者提出了部署诱饵节点间接实现 IP 地址跳变的方法。Jafarian 等人[12]提出了基于 OpenFlow 的随机主机突变 OF-RHM (OpenFlow Random Host Mutation), 实现了对终端透明的 IP 跳变, 降低扫描攻击的有效性。该方法并不直接修改主机的 IP 地址, 而是利用 Openflow 协议频繁切换网络为主机分配的虚拟 IP 地址, 实现动态 IP 通信, 使扫描攻击失效, 实验结果显示该方法可有效抵抗 99%的外部扫描, 保护 90%的主机不受 0-Day 蠕虫攻击。Sun 等人[41]考虑到攻击者有可能在一个跳变周期内完成扫描并发起进一步攻击, 提出了一种诱饵增强型无缝 IP 地址随机化方法, 该方法在网络中部署大量诱饵节点吸引攻击者, 并随机切换受保护主机和诱饵节点的 IP 地址, 防止攻击者识别和排除诱饵节点, 同时利用虚拟网络地址转换迁移正在进行的通信, 保证合法通信不被中断。即使攻击者在一个周期内完成扫描, 其也无法区分真实的主机和诱饵节点, 从而使得网络的安全性得到提高。

在端口信息跳变方面, Shin 等人[33]提出基于“白洞”欺骗的网络 MTD。对于网络扫描攻击, 采用返回信息混淆的方式, 欺骗应答目标系统的所有的端口都是开放的, 使攻击者获取不到有用的信息, 实现移动目标防御的目的。

(2) 指纹跳变

在攻击的早期阶段, 尤其是探测阶段, 会采用指纹欺骗方法, 使攻击者在扫描网络时, 获取错误的网络拓扑信息和可用资源或资产。

指纹跳变主要采用欺骗方法, 有两种实现方式。一种方式是对正常的响应数据包中多个域进行随机修改和替换。Albanese 等人[40]提出了基于图论的指纹欺骗方法, Zhao 等人[42]提出了基于 SDN 的指纹跳变方法, 通过透明拦截和修改响应数据包指纹特征, 变化受保护主机的指纹信息, 使攻击者错误判断目标主机的操作系统, 从而达到驱使攻击者离开受保护主机或者欺骗攻击者发起无效攻击的目的。另一种方式是通过部署类似蜜罐、蜜网等网络诱饵进行网络欺骗, 以呈现给攻击者动态的指纹。Wang 等人[43]提出了种基于 SDN 的扫描反射器(Sniffer Reflector)抵抗网络扫描攻击, 该方法并不阻止扫描流量, 而是将扫描流量反射到一个构建的虚拟影子网络中, 影子网络模拟真实网络设备和服务, 对扫描流量做出应答, 使攻击者不能获取真实网络的内部信息, 难以对网络发起进一步的攻击。Shakarian 等人[44]将移动目标防御和网络诱饵相结合, 提出了一种诱骗防御技术, 在网络中引入 “干扰簇”, 扩大攻击者的探测空间, 降低攻击者获取准确指纹信息的概率。Shi 等人[45]提出了基于 SDN 的移动目标防御系统, 通过在网络中大量部署诱饵服务器, 将可疑流量转发给诱饵服务器, 以此实现指纹跳变。

(3) 虚假路径

Clark 等[46]研究了在无线中继网络中欺骗路由的影响, 并使用两阶段博弈模型建模, 寻求缓解阻塞攻击的解决方案。

4.2 系统层欺骗

系统层欺骗涵盖基于主机的欺骗技术, 其主要应对两种类型的攻击威胁, 外部攻击和内部攻击。

(1) 外部攻击者

检测。Wang 等人[47]提出了多层欺骗框架, 增强系统的检测能力。该框架包含用于用户配置文件, 文件, 服务器, 网络或系统活动的诱饵, 这些诱饵掩盖了系统的真实资产, 并保护他们免受定向攻击。

Rrushi 等人[48]提出了一种类似的方法, 将诱饵网络接口控制器用于 Windows 操作系统。正常的软件不会尝试访问该诱饵接口, 从而可以利用此诱饵接口诱引和检测系统上可能运行的恶意软件。

真伪系统。与之前主要用于增强系统检测能力的欺骗技术对比, Rowe 等人[49]提出了一种主动欺骗的方法, 通过使用伪造的蜜罐, 使真实的系统看起来像蜜罐, 从而使攻击者感到困惑, 令其远离真实的系统。

系统迁移。类似的, Urias 等人[50]提出克隆和迁移受到威胁的计算机系统, 并将其放置在欺骗性环

表 2 基于网络空间欺骗的移动目标防御技术分类

Table 2 Classification of Cyber Deception-Based Moving Target Defense Techniques

分类	威胁或攻击	技术方案		参考文献
网络层欺骗	探测攻击	IP 地址跳变	虚拟 IP 地址	[12]
			诱饵节点	[41]
		端口跳变	“白洞”欺骗	[33]
		指纹跳变	指纹欺骗(图理论)	[40]
			修改响应数据包指纹	[42]
			虚拟影子网络	[43]
			网络诱饵(干扰簇)	[44]
			诱饵服务器 CHAOS	[45]
		虚假路径		[46]
系统层欺骗	外部攻击者	增强检测能力		[47][48]
		真伪系统		[49]
		系统迁移		[50]
		多样化		[51]
	内部攻击者	蜜罐权限		[52]
应用层欺骗	软件妥协	响应延迟		[53]
		软件诱饵		[54]
		蜜糖补丁		[55]
		虚假 gadgets		[56]
		影子蜜罐		[57]
		中间层, 提供虚假视图		[58]
	web 攻击	虚假链接		[27][64]
		虚假配置文件		[30]
		虚假表格		[31]
		虚假 URL 参数		[65]
		虚假 web 页面		[77]
		欺骗即服务		[36][37]
数据层欺骗	身份窃取	虚假账户		[66][67][68]
		虚假密码		[23][70]
		虚假加密		[69]
	数据泄露	诱饵文件		[71]
		诱饵文件的自动分发		[72]
		蜜牌(数据库)		[73]
		虚假源代码		[74]
	隐私侵权	虚假文件		[75][76]

境中, 通过一个复制网络和系统配置以模仿真实的网络环境的欺骗环境。

多样化。Kontaxis 等人[51]建议将整个应用程序服务器进行复制多次, 产生虚假的计算活动。

(2) 内部攻击者

为了检测和缓和内部攻击者的威胁, Kaghazgaran 等人[52]提出通过蜜罐权限扩展基于角色的访问控制。通过将这些伪造的权限分配给虚假的系统资产, 并监视试图访问或修改资产的企图, 从而发现触发这些恶意企图的内部人员。

4.3 应用层欺骗

应用层欺骗涉及特定类的应用程序欺骗技术, 如 web 应用程序或数据库等。主要应对两种类型的威胁, 基于主机的软件妥协和远程的 web 攻击。

(1) 软件妥协

最常用的软件欺骗方法是设计虚假(不存在)的漏洞或随机响应常见的漏洞扫描尝试来欺骗攻击者。

一种直接的欺骗反应是通过随机增加延迟来模拟系统饱和, 从而欺骗潜在的敌手[53]。

Michael 等人[54]引入了软件诱饵的概念, 该诱饵可以检测并响应可疑行为(例如蠕虫与其尝试感染的系统组件之间的交互)。

Araujo 等人[55]将软件补丁转换成虚假的但看似真实的漏洞(也称为“蜜糖补丁”), 这极大地限制了攻击者判断其攻击是否成功的能力。一旦检测到攻击者利用了虚假的漏洞, 系统会无缝衔接地将攻击者转接到此软件的虚假版本。

Crane 等人[56]在代码中引入了伪装成 gadgets 的软件陷阱, 并检测面向返回的编程攻击。一旦这些陷阱被利用, 它们就会检测并发出警报。

Anagnostakis 等人[57]引进了影子蜜罐的概念, 结合了蜜罐和异常检测的特征。影子蜜罐可以是受保护的应用程序(如, web 服务器或客户端)的一个实例, 该实例与真实的应用程序共享所有的内部状态, 但是可以检测并捕获潜在的攻击。由异常检测器错误分类的合法流量也会被影子蜜罐进一步验证并处理。

Taylor 等[58]通过在基本文件系统之上添加中间层, 并在中间层注入诱饵, 从而为不受信任的对象提供虚假的系统视图。

(2) Web 攻击

当前基于 web 应用的 MTD 技术可以分为三类: 动态平台, 随机化和欺骗。动态平台方法主要是在 web 服务器上部署不同的 MTD 方法[59-60] 。随机化方法提供了多个可替换的属性值(如 web 指令集随机化, HTML 元素随机化等)[61-63]。欺骗使用虚假的属性掩盖了攻击面的真实属性, 从而降低了其他属性被攻击的可能性。

Brewer 等人[27]设计了一个嵌入虚假链接的 web 应用程序。这些虚假链接是对普通用户不可见的, 但会被尝试连接访问此应用的爬虫程序或僵尸程序触发。类似的, Gavrilis 等人[64]通过使用嵌入在 web 网

页中诱饵链接检测拒绝服务攻击。

另一种欺骗 web 攻击的方式是使用虚假信息伪装 web 服务器的配置信息。只有恶意用户会尝试访问或利用这些信息。Virvilis 等人[30]引入了虚假配置文件, 如虚假条目, 不可见链接, 虚假 HTML 注释(包含虚假账户信息等), 以检测潜在的攻击者。同时, 利用虚假表格[31], 虚假 URL 参数[65]等显示虚假的配置错误, 从而误导攻击者并保护目标系统。

Han 等人[36]将当前几乎所有的欺骗方法部署在代理服务器上。Daniel Fraunholz 等[37]在反向代理上部署了各种新的基于欺骗的防御机制, 例如版本欺骗, 状态码篡改和虚拟文件等。通过使代理服务器看似易受攻击者的攻击, 诱使攻击者。

4.4 数据层欺骗

数据层欺骗使用虚假的或诱导的数据欺骗攻击者, 主要应对三种类型的威胁, 身份窃取, 数据泄露和隐私侵权。

(1) 身份窃取

虚假账户、虚假密码和虚假加密都使用诱骗数据来阻止攻击者窃取身份信息。虚假账户被用来追踪攻击者[66], 检测恶意软件[67]。Lazarov 等人[68]通过创建五个虚假的谷歌电子表格, 包含诱饵银行信息、电汇信息等, 帮助研究人员追踪并调研恶意攻击者使用这些数据的行动轨迹。欺骗技术也被用来保护用户的密码。为了保护被泄露的哈希之后的用户密码, Juels 等人[23]引入了虚假密码(honeywords)来掩盖真实的授权密码。之后, 又提出了虚假加密的技术[69], 当使用不正确的密钥或密码解密某个密文时, 会产生一个看起来有效的诱饵信息。Bojinov 等人[70]提出了防盗密码管理器的概念, 在客户端随机生成新的密码实例。

(2) 数据泄露

包含蜜标、蜜牌的诱导文件可以在被打开时触发警报, 从而防止数据泄露。Salem 等人[71]研究了诱饵文件用于伪装攻击检测的作用。Voris 等人[72]专注于诱饵文件的自动分发, 以增加发现内部攻击者的概率。Cenys 等[73]在数据库中引入模仿敏感信息的蜜牌, 检测获取非授权访问数据的攻击者。Park 等[74]通过生成虚假的但看似可信的 Java 源代码检测越权访问的攻击者。

(3) 隐私侵权

Nikiforakkis 等人[75]和 Liu 等人[76]使用在访问或修改时触发警报的虚假文件, 检测在 web 托管提供商和对等网络上共享的文档的隐私侵权行为。

Kapravelo 等人[77]使用虚假 web 页面, 根据浏览器扩展程序的期望来调整页面结构和内容, 从而以浏览器扩展程序中侵犯隐私的形式识别恶意行为。

5 基于网络空间欺骗的度量和评估

基于不同的设计准则和期望实现的目标, 评估的标准也不同。例如, 可以评价欺骗技术的合理性, 可检测性, 可变性, 可区分性, 保密性等。尽管这些度量属性在欺骗的应用部署中起着重要的作用, 但是大多数属性都难以形式化和量化, 从而使基于欺骗的量化评估非常具有挑战性。

本文主要总结与评价基于欺骗的有效性的评估方法。为此, 文章将评估欺骗技术的有效性方法主要分为两类, 一是基于理论模型; 二是基于实验仿真, 分别对在可控的环境下, 只有很少的参与者参与的情境下进行评估; 或是对在真实环境下, 将欺骗技术公开, 针对真实用户和攻击者的情景进行评估。

5.1 基于理论模型

理论模型主要是提出某种方法论(如概率模型, 基于攻击图的模型, 也可以是一个过程, 亦或是博弈论模型), 设计在计算机系统中何时, 何地, 如何集成欺骗技术。Markov[78-80]、博弈论[81]、攻击图[82-83]等均是 MTD 评估的主要手段。而如何度量欺骗在 MTD 目标系统的行为, 是网络空间欺骗研究的关键问题。对攻击者行为对象的度量可以帮助系统确定是否陷入攻击, 对防御者行为的度量可以帮助系统确定更有效的防御欺骗策略。

概率模型基于概率论来评估欺骗的收益和成本。由于攻击者相信计算机系统会告诉他们真相, 因此系统说谎或误导可能是有效的。为此, Rowe 等人[84]通过计算机中通用的理由, 如系统崩溃、通信中断等欺骗攻击者, 并利用概率性模型评估攻击者对虚假理由的信任情况, 以及攻击者对自己是否受到欺骗的怀疑情况。模型有助于防御者计划何时以及如何欺骗, 同时监视攻击者对所提供的理由的信任情况。

Crouse 等人[85]将超几何分布模型用于研究计算机网络中不同种类防御方法的有效性, 包括无保护措施, 采用欺骗(蜜罐)的防御措施, 以及地址随机化。他们发现欺骗(蜜罐)方法比地址随机化方法更成功, 但同时使用两者能更大程度地增加安全性。

攻击图是同时考虑目标系统的脆弱性、攻击目标和节点连接性, 描述导致系统状态转移的复杂攻击序列的一种方法。Cohen 等人[86]建模了攻击者可能妥协计算机系统的过程与路径, 并在攻击图中引入虚假的目标, 研究如何引诱攻击者远离真实的目标。

博弈论描述攻击者与防御者之间的交互, 建模

并计算最优的防御策略。Feng 等人[87]提出可以通过主动地泄露信息进一步地提升 MTD 的安全性。其提出将信号博弈用于移动目标防御。防御者主动向攻击者释放虚假信号影响攻击者的决策和行动, 增加攻击者的成本。Carroll 等人[88]基于博弈理论, 在攻击者与防御者对彼此不完全了解的情况下, 建立了欺骗影响攻防交互的模型。在博弈中, 防御者可以采取两种欺骗防御方案, 一是将合法服务器隐藏为蜜罐, 二是使蜜罐看起来像合法服务器。为了防止远程攻击者获取操作系统指纹, Rahman 等人[89]使用信号博弈, 欺骗并扰乱攻击者探测的结果。进一步地, Clark 等人[90]建模了攻击者能够识别真实和虚假节点的延迟, 分析了欺骗防御场景下 IP 地址随机化的最优防御策略。Han 等人[36]提出了通过贝叶斯博弈用于异常检测; 为了更好地评估欺骗的效果, 研究人员进行了 150 个用户参与实验, 通过检测误报率、漏报率评估欺骗的有效性, 发现欺骗可以检测到攻击者, 但是仍有 36%的攻击者成功利用了漏洞, 而没有触发欺骗的陷阱。

当前众多学者结合移动目标防御的思想提出了形式各样的基于攻击面的转移方案, 但基于网络空间欺骗的 MTD 研究仍没有体系化的理论模型支撑。因此分析各欺骗技术或欺骗属性, 归纳抽象网络空间欺骗技术的关键因素, 将会是将来研究的重要工作。

5.2 基于实验仿真

本文主要总结了基于不同欺骗层次, 不同欺骗技术的实验环境部署, 以便后续对欺骗的研究奠定基础。

5.2.1 基于可控环境

不同的实验设置, 不用的评估策略均被用于评估欺骗的有效性, 依据欺骗的作用范围, 分别从网络层、系统层、应用层和数据层, 总结和评价基于欺骗的技术的有效性。

网络层。Cohen 等人[91]基于仿真的攻击图, 评估了基于网络的欺骗防御的有效性。实验邀请了少量学生和安全专家参与。将参与方分为两组, 一组不知道欺骗技术的存在, 另一组被告知欺骗技术的存在。结果表明, 基于网络的欺骗技术真实有效, 因为攻击者需要耗费更多的时间试图通过欺骗的路径而不是真实的攻击路径。

进一步地, Cohen 等人[86]引入了一个更泛化的攻击图模型, 以虚假目标诱引攻击者。实验邀请了七名学生, 并被要求攻击并试图破坏系统。结果表明, 攻击者被不断地误导, 并按照虚假的攻击路径攻击。

Al-Shaer 等人[92]提出了一种随机主机突变方法, 通过在不牺牲网络完整性、可管理性或性能的情况下, 以一种智能和不可预测的方式随机地改变终端主机的虚拟 IP 地址, 而保持真实的 IP 地址不变, 将终端主机变成不可跟踪的移动目标。此方法可以无缝地部署在任何现有网络中, 而不需要对终端主机或网络基础设施进行任何更改, 同时保持对端主机的透明性。

系统层。Heckman 等人[93]组织了一场红蓝队伍对抗的攻防博弈。蓝队的任务目标是建立一个指挥控制系统, 并保护该系统免受红队攻击。蓝队尝试了多种欺骗手段误导攻击者。实验表明, 欺骗技术对红队的攻击产生了重大影响, 因为红队耗费更多时间试图攻击破坏虚假目标。

应用层。Araujo 等人[55]提出蜜糖补丁的概念来缓和对已知漏洞的攻击。在包含 Apache HTTP 服务器和仿真的 web 应用程序的实验环境下, 根据真实的漏洞可以转化为蜜糖漏洞的数量评估了该方法的有效性。在收集的 75 个漏洞中, 有 49 个漏洞(大约 65%)可以转化为蜜糖补丁。

Han 等人[36]评估了可用于检测 web 攻击的现有的欺骗技术, 包括虚假参数, 虚假账户, 虚假陷阱资源等。作者利用 CTF 比赛, 要求 150 名参与者在一个专门设计的电子商务程序中发现漏洞, 其中有 64%的参与者成功发现了至少一个漏洞。

数据层。数据层的欺骗技术主要是产生并放置诱导的用户账号或用户文件, 评估方法的有效性主要是使参与者辨别并区分真实的数据与虚假的数据。

Yuill 等人[94]将诱饵文件部署在蜜网上进行测试, 并邀请一组学生参与并尝试攻击系统。结果表明诱饵文件可以检测至少一个攻击者, 且攻击者在触发警报前没有意识到诱饵文件的存在。此外, 最有效的诱饵文件是部署在文件系统根目录附近的文件。

5.2.2 基于真实环境

Borders 等人[95]评估了诱饵 IP 地址误导远程攻击者的有效性。为此, 作者设计了一个实验平台 OpenFire, 其包含一个 OpenFire 网关, 用来拦截外部请求, 并将其重定向到其他真实或虚假的主机上。如果一个网络数据包请求真实服务, 则将其转发到相应的主机。如果数据包的目的地是真实主机上不存在的服务或未使用的 IP 地址, 则将其转发到一个诱饵。实验表明, 使用欺骗配置比正常配置下, 攻击者成功的次数减少了 65%。

为了评估诱饵文件的有效性, Nikiforakis 等人[75]将诱饵文件上传到 100 个公共文件托管服务中。一

表 3 基于欺骗的移动目标防御评估方法分类

Table 3 Overview of Deceptive Moving Target Defense Evaluation Methodologies

分类	方案	参考文献	实验对象	度量
基于理论模型	概率模型	[84][85]		攻击者对虚假理由的信任
	攻击图	[82][83][86]		
	博弈论	[36][1][81][87][88][89]		最优防御策略
基于可控环境	网络层	[91]	27 名学生	攻击的持久度
		[86]	7 名学生	控制攻击路径的能力
		[92]	100 Nmap	真实 IP 被发现的概率
	系统层	[93]	4 个红蓝队伍	用户的反应
	应用层	[55]		实用性
		[36]	150 CTF 比赛者	检测到漏洞的人员数量
	数据层	[94]	3 名学生	检测到攻击者的数量
基于真实环境		[95]	潜在的攻击者	攻击成功的次数
		[75]	潜在的攻击者	隐私侵犯检测

个月的时间内, 有 80 个 IP 地址访问了诱饵文件, 并触发了警报。诱饵文件中包含虚假的证书, 可以使得远程用户连接到为实验目的设计实现的虚假 web 应用程序。实验中, 有来自 43 个 IP 地址的敌手成功登录了 93 次, 虚假账户信息在诱饵文档中被泄露。

6 关键技术研究展望

网络空间欺骗由于其多样化的变化形式为 MTD 系统提供了增加属性攻击面转换空间的手段, 提高了 MTD 的防御熵。具有的优势如下:

(1) 改变攻击者对目标系统的认知, 影响攻击者的入侵行为, 使之按照防御者的意志进行选择。网络空间欺骗的主要目的是使攻击者相信目标系统存在可利用的、有价值的资源, 转移攻击者的注意力, 将攻击者引向这些虚假的资源。欺骗显著地增加了攻击者的攻击复杂度和不确定性, 使攻击者无法确认其攻击是否有效。

(2) 检测并追踪攻击者的入侵行为轨迹。传统的安全机制主要是通过在网络系统周围创建边界, 阻止非法访问。经典 MTD 不依赖于先验知识, 而是通过利用目标系统的复杂性, 动态地改变系统的配置, 增加攻击者的攻击难度。而欺骗可以为针对系统的网络攻击, 系统攻击面的变化等行为, 提供早期检测, 通过收集攻击者的动机、攻击工具、攻击技术等信息, 分析攻击者的意图, 使防御者提前修补系统漏洞, 或转移攻击面属性, 达到主动防御的目的。

(3) 消耗攻击者的资源, 增加攻击的成本。欺骗可以通过更改真实的目标系统属性特征, 将其伪装成看似虚假的资源, 欺骗攻击者; 或通过伪造的资源, 如蜜网、诱饵文件等, 诱骗攻击者, 吸引攻击者的注意力。因此, 攻击者必须从这些虚假的资源中, 辨别真实的目标, 从而被迫浪费时间与资源, 不得不多次重新探测、攻击或完全放弃攻击。

基于欺骗的动态防御技术进一步改变了网络空间攻防不对称的格局, 是 MTD 研究和发展的重要方向, 但仍存在以下挑战:

多重、多阶段欺骗 MTD 技术，欺骗 MTD 技术的研究涉及到计算机系统和网络体系结构的各个层次, 本文总结了在不同层次, 针对不同的威胁, 提出了各种各样的基于欺骗的动态防御技术。而分析各欺骗技术的相互影响与关系, 判断不同的欺骗技术能否叠加使用, 实现多种欺骗技术整合, 从而形成一个完整的欺骗MTD防御体系是未来亟待解决的问题。此外, 当前基于欺骗 MTD 的防御技术主要用于抵御攻击的不同阶段的威胁, 如探测阶段。如何实现各攻击阶段欺骗 MTD 技术的融合, 提高系统的整体防御能力是将来重要的研究方向。

动态的欺骗 MTD 技术。欺骗 MTD 主要是通过创建欺骗攻击面, 更改攻击者对系统的认知。欺骗 MTD 是攻防双方的博弈, 防御者需要实时关注攻击者的状态, 从而动态调整欺骗方案。随着攻防博弈的演进, MTD 系统中进行欺骗的资源或信号若长期保持不变, 欺骗防御的作用会不断衰减。因此, 探讨欺骗元素的动态化技术, 应对攻击行为的动态变化至关重要。

自动化的欺骗 MTD 技术。任何尝试连接欺骗资源的访问都被视为异常访问, 因此基于欺骗的动态防御技术可以实现各种自动化的事件响应, 从而使目标系统提前转移攻击面属性, 抵御攻击。但在实现自动化地部署和维护欺骗时, 仍存在挑战。如何自动

化地分析目标系统环境, 如何自动化地生成诱饵, 以及如何自动化地部署欺骗均是亟待解决的问题。

智能化的欺骗 MTD 技术 随着安全需求的不断变化, 如何应对愈加智能化的攻击手段是安全防御的重要问题。随着人工智能或机器学习等新兴技术在网络空间安全领域的不断发展应用, 可为欺骗MTD技术带来改观。将这些新兴技术引入欺骗MTD, 提高防御技术的学习能力、自适应能力和行为决策能力是未来可能的研究方向。

参考文献

[1] Jajodia S, Ghosh A K, Swarup V, et al. Moving Target Defense: Creating Asymmetric Uncertainty for Cyber Threats[M]. New York, NY: Springer New York, 2011.

[2] Zhu Q Y, Başar T. Game-Theoretic Approach to Feedback-Driven Multi-Stage Moving Target Defense[C]. *GameSec 2013*: *4th International Conference on Decision and Game Theory for Security - Volume 8252*, 2013: 246-263.

[3] Pingree L. Emerging technology analysis: Deception techniques and technologies create security technology business opportuni-ties. Gartner, Inc, 2015.

[4] Stoll C. The cuckoo's egg: tracking a spy through the maze of computer espionage[M]. New York: Doubleday, 1989

[5] Ammann P E, Knight J C. Data Diversity: An Approach to Software Fault Tolerance[J]. *IEEE Transactions on Computers*, 1988, 37(4): 418-425.

[6] Man Y, Yin Q, Zhu X, et al. Fine-grained data randomization technique based on field-sensitive pointer analysis [J]. Journal of Computer Applications, 2016.

[7] Temizkan O, Park S, Saydam C. Software Diversity for Improved Network Security: Optimal Distribution of Software-Based Shared Vulnerabilities[J]. *Information Systems Research*, 2017, 28(4): 828-849.

[8] Forrest S, Somayaji A, Ackley D H. Building Diverse Computer Systems[C]. *The Sixth Workshop on Hot Topics in Operating Systems*(*Cat*. *No*.*97TB100133*), 2002: 67-72.

[9] Thimbleby H. Can Viruses ever be Useful?[J]. *Computers & Security*, 1991, 10(2): 111-114.

[10] Pappas V, Polychronakis M, Keromytis A D. Smashing the Gadgets: Hindering Return-Oriented Programming Using In-Place Code Randomization[C]. *2012 IEEE Symposium on Security and Privacy*, 2012: 601-615.

[11] Koo H, Polychronakis M. Juggling the Gadgets: Binary-Level Code Randomization Using Instruction Displacement[C]. *The 11th ACM on Asia Conference on Computer and Communications Security*, 2016: 23-34.

[12] Jafarian J H, Al-Shaer E, Duan Q. Openflow Random Host Mutation: Transparent Moving Target Defense Using Software Defined Networking[C]. *The first workshop on Hot topics in software defined networks*, 2012: 127-132.

[13] Wang S L, Zhang L, Tang C J. A New Dynamic Address Solution for Moving Target Defense[C]. *2016 IEEE Information Technology, Networking, Electronic and Automation Control Conference*, 2016: 1149-1152.

[14] 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: 263-270.

[15] Thompson M, Evans N, Kisekka V. Multiple OS Rotational Environment an Implemented Moving Target Defense[C]. *2014 7th International Symposium on Resilient Control Systems*, 2014: 1-6.

[16] 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.

[17] Kirrmann H, Dzung D. Selecting a Standard Redundancy Method for Highly Available Industrial Networks[C]. *2006 IEEE International Workshop on Factory Communication Systems*, 2006: 386-390.

[18] Al-Wakeel S S, AL-Swailem S A. PRSA: A Path Redundancy Based Security Algorithm for Wireless Sensor Networks[C]. *2007 IEEE Wireless Communications and Networking Conference*, 2007: 4156-4160.

[19] Yuan E, Malek S, Schmerl B, et al. Architecture-Based Self-Protecting Software Systems[C]. *The 9th international ACM Sigsoft conference on Quality of software architectures*, 2013: 33-42.

[20] Chang F W, Ji M, Leung S T, et al. Myriad: Cost-Effective Disaster Tolerance[C]. *FAST*, 2002, 2: 8.

[21] Gorbenko A, Kharchenko V, Romanovsky A. Using Inherent Service Redundancy and Diversity to Ensure Web Services Dependability[M]. Methods, Models and Tools for Fault Tolerance. Berlin, Heidelberg: Springer, 2009: 324-341.

[22] Bell J B, Whaley B. Cheating and deception[M]. New Brunswick, NJ: Transaction Publishers, 1991.

[23] Juels A, Rivest R L. Honeywords: Making Password-Cracking Detectable[C]. *The 2013 ACM SIGSAC conference on Computer & communications security*, 2013: 145-160.

[24] Provos N. Honeyd-a virtual honeypot daemon[C]. *The 10th DFN-CERT Workshop*, Hamburg, Germany. 2003, 2: 4.

[25] Li S J, Schmitz R. A Novel Anti-Phishing Framework Based on Honeypots[C]. *2009 eCrime Researchers Summit*, 2009: 1-13.

[26] Yue C, Wang H N. BogusBiter: A Transparent Protection Against Phishing Attacks[J]. *ACM Transactions on Internet Technology*, 2010, 10(2): 1-31.

[27] Brewer D, Li K, Ramaswamy L, et al. A Link Obfuscation Service to Detect Webbots[C]. *2010 IEEE International Conference on Services Computing*, 2010: 433-440.

[28] Takabi H, Jafarian J H. Insider Threat Mitigation Using Moving Target Defense and Deception[C]. *The 2017 International Workshop on Managing Insider Security Threats*, 2017: 93-96.

[29] Takabi H, Jafarian J H. Insider Threat Mitigation Using Moving Target Defense and Deception[C]. *The 2017 International Workshop on Managing Insider Security Threats*, 2017: 93-96.

[30] Virvilis N, Vanautgaerden B, Serrano O S. Changing the Game: The Art of Deceiving Sophisticated Attackers[C]. *2014 6th International Conference on Cyber Conflict*, 2014: 87-97.

[31] Katsinis C, Kumar B. A Framework for Intrusion Deception on

Web Servers[C]. *International Conference on Internet Computing*, ICOMP'13. 2013.

[32] Bercovitch M, Renford M, Hasson L, et al. HoneyGen: An Automated Honeytokens Generator[C]. *2011 IEEE International Conference on Intelligence and Security Informatics*, 2011: 131-136.

[33] Shin S, Yegneswaran V, Porras P, et al. AVANT-GUARD: Scalable and Vigilant Switch Flow Management in Software-Defined Networks[C]. *The 2013 ACM SIGSAC conference on Computer & communications security*, 2013: 413-424.

[34] Al-Shaer E. Toward Network Configuration Randomization for Moving Target Defense[M]. Moving Target Defense. New York: Springer, 2011: 153-159.

[35] Borders K, Zhao X, Prakash A. Siren: Catching Evasive Malware[C]. *2006 IEEE Symposium on Security and Privacy*, 2006: 6pp.-85.

[36] Han X, Kheir N, Balzarotti D. Evaluation of Deception-Based Web Attacks Detection[C]. *The 2017 Workshop on Moving Target Defense*, 2017: 65-73.

[37] Fraunholz D, Reti D, Anton S D, et al. Cloxy: A Context-Aware Deception-As-a-Service Reverse Proxy for Web Services[C]. *The 5th ACM Workshop on Moving Target Defense*, 2018: 40-47.

[38] Manadhata P K, Wing J M. An Attack Surface Metric[J]. *IEEE Transactions on Software Engineering*, 2011, 37(3): 371-386.

[39] Manadhata P K, Wing J M. A Formal Model for a System's Attack Surface[M]. Moving Target Defense. New York: Springer, 2011: 1-28.

[40] Albanese M, Battista E, Jajodia S. Deceiving Attackers by Creating a Virtual Attack Surface[M]. Cyber Deception. Cham: Springer, 2016: 167-199.

[41] Sun J H, Sun K. DESIR: Decoy-Enhanced Seamless IP Randomization[C]. *IEEE INFOCOM 2016 - The 35th Annual IEEE International Conference on Computer Communications*, 2016: 1-9.

[42] Zhao Z, Liu F L, Gong D F. An SDN-Based Fingerprint Hopping Method to Prevent Fingerprinting Attacks[J]. *Security and Communication Networks*, 2017, 2017: 1-12.

[43] Wang L, Wu D H. Moving Target Defense Against Network Reconnaissance with Software Defined Networking[C]. *International Conference on Information Security*. Cham: Springer, 2016: 203-217.

[44] Shakarian P, Kulkarni N, Albanese M, et al. Keeping Intruders at Bay: A Graph-theoretic Approach to Reducing the Probability of Successful Network Intrusions[C]. *International Conference on E-Business and Telecommunications*. Cham: Springer, 2015: 191-211.

[45] Shi Y, Zhang H G, Wang J, et al. CHAOS: An SDN-Based Moving Target Defense System[J]. *Security and Communication Networks*, 2017, 2017: 1-11.

[46] Clark A, Zhu Q Y, Poovendran R, et al. Deceptive Routing in Relay Networks[C]. *International Conference on Decision and Game Theory for Security*. Berlin, Heidelberg: Springer, 2012: 171-185.

[47] Wang W, Bickford J, Murynets I, et al. Detecting Targeted Attacks by Multilayer Deception[J]. *Journal of Cyber Security and Mobility*, 2013, 2(2): 175-199.

[48] Rrushi J L. NIC Displays to Thwart Malware Attacks Mounted from within the OS[J]. *Computers & Security*, 2016, 61: 59-71.

[49] Rowe, Duong, Custy. Fake Honeypots: A Defensive Tactic for Cyberspace[C]. *2006 IEEE Information Assurance Workshop*, 2006: 223-230.

[50] Urias V E, Stout W M S, Lin H W. Gathering Threat Intelligence through Computer Network Deception[C]. *2016 IEEE Symposium on Technologies for Homeland Security*, 2016: 1-6.

[51] Kontaxis G, Polychronakis M, Keromytis A D. Computational Decoys for Cloud Security[M]. Secure Cloud Computing. New York: Springer, 2014: 261-270.

[52] Kaghazgaran P, Takabi H. Toward an Insider Threat Detection Framework Using Honey Permissions[J]. *J Internet Serv Inf Secur*, 2015, 5(3): 19-36.

[53] Julian D P. Delaying-type responses for use by software decoys[R]. NAVAL POSTGRADUATE SCHOOL MONTEREY CA, 2002.

[54] Michael J B, Auguston M, Rowe N C, et al. Software decoys: Intrusion detection and countermeasures[R]. NAVAL POSTGRADUATE SCHOOL MONTEREY CA DEPT OF COMPUTER SCIENCE, 2002.

[55] Araujo F, Hamlen K W, Biedermann S, et al. From Patches to Honey-Patches: Lightweight Attacker Misdirection, Deception, and Disinformation[C]. *The 2014 ACM SIGSAC Conference on Computer and Communications Security*, 2014: 942-953.

[56] Crane S, Larsen P, Brunthaler S, et al. Booby Trapping Software[C]. *The 2013 New Security Paradigms Workshop*, 2013: 95-106.

[57] Anagnostakis K G, Sidiroglou S, Akritidis P, et al. Detecting targeted attacks using shadow honeypots[C]. 14th Usenix Security Symposium, 2005.

[58] Taylor T, Araujo F, Kohlbrenner A, et al. Hidden in Plain Sight: Filesystem View Separation for Data Integrity and Deception[C]. *International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment*. Cham: Springer, 2018: 256-278.

[59] Jia Q, Sun K, Stavrou A. MOTAG: Moving Target Defense Against Internet Denial of Service Attacks[C]. *2013 22nd International Conference on Computer Communication and Networks*, 2013: 1-9.

[60] Huang Y, Sood A, Bhaskar R K. Countering web defacing attacks with system self-cleansing[C]. *7th Word Multiconference on Systemics, Cybernetics and Informatics*. 2003: 12-16.

[61] Niakanlahiji A, Jafarian J H. WebMTD: Defeating Web Code Injection Attacks Using Web Element Attribute Mutation[C]. *The 2017 Workshop on Moving Target Defense*, 2017: 17-26.

[62] Christodorescu M, Fredrikson M, Jha S, et al. End-to-End Software Diversification of Internet Services[M]. Moving Target Defense. New York: Springer, 2011: 117-130.

[63] Vikram S, Yang C, Gu G F. NOMAD: Towards Non-Intrusive Moving-Target Defense Against Web Bots[C]. *2013 IEEE Conference on Communications and Network Security*, 2013: 55-63.

[64] Gavrilis D, Chatzis I, Dermatas E. Flash Crowd Detection Using Decoy Hyperlinks[C]. *2007 IEEE International Conference on Networking, Sensing and Control*, 2007: 466-470.

[65] Robert Petrunić A B. Honeytokens as Active Defense[C]. *2015 38th International Convention on Information and Communication*

Technology, *Electronics and Microelectronics*, 2015: 1313-1317.

[66] McRae C M, Vaughn R B. Phighting the Phisher: Using Web Bugs and Honeytokens to Investigate the Source of Phishing Attacks[C]. *2007 40th Annual Hawaii International Conference on System Sciences*, 2007: 270c.

[67] Akiyama M, Yagi T, Aoki K, et al. Active Credential Leakage for Observing Web-Based Attack Cycle[C]. *International Workshop on Recent Advances in Intrusion Detection*. Berlin, Heidelberg: Springer, 2013: 223-243.

[68] Lazarov M, Onaolapo J, Stringhini G. Honey Sheets: What Happens to Leaked Google Spreadsheets? [C]. *The 9th USENIX Conference on Cyber Security Experimentation and Test*, 2016: 3.

[69] Juels A. A Bodyguard of Lies: The Use of Honey Objects in Information Security[C]. *The 19th ACM symposium on Access control models and technologies*, 2014: 1-4.

[70] Bojinov H, Bursztein E, Boyen X, et al. Kamouflage: Loss-Resistant Password Management[C]. *European Symposium on Research in Computer Security*. Berlin, Heidelberg: Springer, 2010: 286-302.

[71] Ben Salem M, Stolfo S J. Decoy Document Deployment for Effective Masquerade Attack Detection[C]. *International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment*. Berlin, Heidelberg: Springer, 2011: 35-54.

[72] Voris J, Jermyn J, Boggs N, et al. Fox in the Trap: Thwarting Masqueraders via Automated Decoy Document Deployment[C]. *The Eighth European Workshop on System Security*, 2015: 1-7.

[73] Cenys A, Rainys D, Radvilavius L, et al. Implementation of honeytoken module in dbms oracle 9ir2 enterprise edition for internal malicious activity detection[J]. IEEE Computer Society's TC on Security and Privacy, 2005: 1-13.

[74] Park Y, Stolfo S J. Software Decoys for Insider Threat[C]. *The 7th ACM Symposium on Information*, *Computer and Communications Security*, 2012: 93-94.

[75] Nikiforakis N, Balduzzi M, Van Acker S, et al. Exposing the Lack of Privacy in File Hosting Services[C]. *The 4th USENIX conference on Large-scale exploits and emergent threats*, 2011: 1.

[76] Liu B S, Liu Z Y, Zhang J Y, et al. How many Eyes are Spying on your Shared Folders? [C]. *The 2012 ACM workshop on Privacy in the electronic society*, 2012: 109-116.

[77] Kapravelos A, Grier C, Chachra N, et al. Hulk: Eliciting malicious behavior in browser extensions[C]. *23rd USENIX Security Symposium*. 2014: 641-654.

[78] Zhuang R, DeLoach S A, Ou X M. Towards a Theory of Moving Target Defense[C]. *The First ACM Workshop on Moving Target Defense*, 2014: 31-40.

[79] Maleki H, Valizadeh S, Koch W, et al. Markov Modeling of Moving Target Defense Games[C]. *The 2016 ACM Workshop on Moving Target Defense*, 2016: 81-92.

[80] 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.

[81] Manadhata P K. Game Theoretic Approaches to Attack Surface Shifting[C]. *Moving Target Defense II*. New York: Springer, 2013: 1-13.

[82] 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.

[83] Hamlet J R, Lamb C C. Dependency Graph Analysis and Moving Target Defense Selection[C]. *The 2016 ACM Workshop on Moving Target Defense*, 2016: 105-116.

[84] Rowe N C. Designing Good Deceptions in Defense of Information Systems[C]. *20th Annual Computer Security Applications Conference*, 2005: 418-427.

[85] Crouse M, Prosser B, Fulp E W. Probabilistic Performance Analysis of Moving Target and Deception Reconnaissance Defenses[C]. *The Second ACM Workshop on Moving Target Defense*, 2015: 21-29.

[86] Cohen F, Koike D. Leading Attackers through Attack Graphs with Deceptions[J]. *Computers & Security*, 2003, 22(5): 402-411.

[87] 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*, 2017: 1-9.

[88] Carroll T E, Grosu D. A Game Theoretic Investigation of Deception in Network Security[C]. *2009 Proceedings of 18th International Conference on Computer Communications and Networks*, 2009: 1-6.

[89] Rahman M A, Manshaei M H, Al-Shaer E. A Game-Theoretic Approach for Deceiving Remote Operating System Fingerprinting[C]. *2013 IEEE Conference on Communications and Network Security*, 2013: 73-81.

[90] Clark A, Sun K, Bushnell L, et al. A Game-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.

[91] Cohen F, Marin I, Sappington J, et al. Red teaming experiments with deception technologies[J]. *IA Newsletter*, 2001.

[92] Al-Shaer E, Duan Q, Jafarian J H. Random Host Mutation for Moving Target Defense[C]. *International Conference on Security and Privacy in Communication Systems*. Berlin, Heidelberg: Springer, 2013: 310-327.

[93] Heckman K E, Walsh M J, Stech F J, et al. Active Cyber Defense with Denial and Deception: Acyber-Wargame Experiment[J]. *Computers & Security*, 2013, 37: 72-77.

[94] Yuill J, Zappe M, Denning D, et al. Honeyfiles: Deceptive Files for Intrusion Detection[C]. *Proceedings from the Fifth Annual IEEE SMC Information Assurance Workshop*, 2005: 116-122.

[95] Borders K, Falk L, Prakash A. OpenFire: Using Deception to Reduce Network Attacks[C]. *2007 Third International Conference on Security and Privacy in Communications Networks and the Workshops - SecureComm*, 2008: 224-233.

张雅勤 于 2015 年在山东大学计算机科学与技术专业获得学士学位。现在中国科学院大学信息工程研究所网络空间安全专业攻读博士学位。研究领域为网络空间安全、移动目标防御、web 安全。Email: zhangyaqin@ iie.ac.cn

Xiaoyan Sun 于 2016 年在美国宾夕法尼亚州立大学信息学专业获得博士学位。现任美国加利福尼亚州立大学萨克拉门托分校计算机科学系助理教授。研究领域为网络安全, 研究兴趣包括: 企业网络安全、入侵检测、数字取证等。Email: xiaoyan.sun@csus.edu

刘峰 于 2009 年在中国科学院软件研究所信息安全国家重点实验室信息安全专业获得博士学位。现任中国科学院信息工程研究所研究员。研究领域为网络空间安全、信息对抗。Email: liufeng@iie.ac.cn

马多贺 于 2015 年在中国科学院信息工程研究所信息安全国家重点实验室获得博士学位。现任中国科学院信息工程研究所副研究员。CCF 高级会员, CISSP。研究领域为移动目标防御、智能安全、网络与系统安全。Email: maduohe@iie.ac.cn

周川 于 2019 年在哈尔滨工业大学通信工程专业获得学士学位。现在中国科学院大学信息工程研究所网络空间安全专业攻读硕士学位。研究领域为移动目标防御、人工智能安全。Email: zhouchuan1@iie.ac.cn