基于动态伪装技术的网络安全防御系统研究

丁朝晖，张　伟，杨国玉
（中国大唐集团科学技术研究院，北京 100043）

摘　要： 伴随着物联网、云计算、大数据、移动互联、人工智能等新技术的迅猛发展，随之而来的安全问题也更加严重，越来越多的未知攻击和未知漏洞使得传统的网络安全防御手段难以适应。基于动态伪装技术的网络安全防御系统原理是通过动态变化的漏洞、缺陷和后门的种类、数量和系统特征等元素构建系统外在特征不确定性的假象，从而实现隐蔽真实的信息系统漏洞、缺陷和后门的目的。

关键词： 动态伪装技术；安全防御系统；网络安全
中图分类号： TN915.08　　**文献标识码：** A　　DOI：10.16157/j.issn.0258-7998.211522

中文引用格式： 丁朝晖，张伟，杨国玉. 基于动态伪装技术的网络安全防御系统研究[J]. 电子技术应用，2022，48(1)：129-132.
英文引用格式： Ding Zhaohui，Zhang Wei，Yang Guoyu. Research on network security defense system based on dynamic camouflage technology[J]. Application of Electronic Technique，2022，48(1)：129-132.

Research on network security defense system based on dynamic camouflage technology

Ding Zhaohui，Zhang Wei，Yang Guoyu
（China Datang Corporation Science and Technology Research Institute，Beijing 100043，China）

Abstract： With the rapid development of Internet of Things，cloud computing，big data，mobile Internet，artificial intelligence and other new technologies，the following security problems are more serious. More and more unknown attacks and vulnerabilities make the traditional network security defense methods difficult to adapt. The principle of network security defense system based on dynamic camouflage technology is to construct the false appearance of the uncertainty of the external characteristics of the system by dynamically changing the types，quantity and characteristics of loopholes，defects and backdoors，so as to achieve the purpose of concealing the real loopholes，defects and backdoors of the information system.

Key words： dynamic camouflage technology；security defense system；network security

0 引言

在当今信息化的时代，物联网、云计算、大数据、移动互联、人工智能、工业控制系统等新技术的出现使得人们的生活变得更加便利和舒适，这些新技术正在迅速占领着人类社会的方方面面，其所应用领域不仅深刻影响着人们的日常生活，而且关系到各个国家的命脉。与此同时，网络空间的安全问题不容忽视，新技术应用的规模越庞大，网络空间的安全问题越严峻，网络安全风险空前巨大[1]。而且，随着新技术应用的深入，越来越多的安全问题是未知的，带来的影响也是未知，这种“未知的未知风险”如同达摩克利斯之剑，随时都有爆发的可能。为此，突破目前静态、被动的安全防御技术的局限性，研究动态、主动的安全防御系统已成为网络安全领域重要的研究方向。

1 网络安全现状分析

从网络安全的整体情况来看，有两个方面的安全难题一直困扰着网络安全防御者。一方面，暴露在互联网上的安全漏洞和后门不计其数，绝大多数漏洞和后门是未知的。迄今为止，尚未形成穷尽复杂信息系统漏洞和彻查后门的理论与方法。从网络防御者角度来看，攻击者利用未知漏洞或后门实施的攻击具备极强的隐蔽性，防御者无法知晓攻击者经过何种途径、通过什么方法进入被防御系统。因此，防御者使用当前的技术手段无法有效防御这种未知的威胁。另一方面，在信息技术全球化的今天，系统中各种软硬件的设计与开发过程中，不可能做到毫无瑕疵，出现缺陷、漏洞或后门的概率极大，而且随着时间的推移，还会暴露出更多更严重的缺陷、漏洞或后门[2]。

就算这些缺陷、漏洞和后门能被防御者所探测或感知。但是，由于种种原因无法将全部缺陷、漏洞和后门完全修复，这也造成了传统的安全扫描和渗透测试技术难以完全发挥其作用，无法实现对已知缺陷、漏洞和后门

的完全修复和清除。

目前,传统的网络防御以“筑高墙、堵漏洞、打补丁”为主,不断地挖掘漏洞、检测后门、寻找缺陷,不断地修补安全漏洞、缺陷与后门,通过不停地防恶意代码、封门堵漏等被动的博弈方式来自我完善。在这种情况下,形成了“易攻难守”的网络安全现状。

在缺陷、漏洞和后门无法完全修复和清除的背景下,亟需一种打破传统安全防御观念的新安全思路,研究用动态伪装技术来掩盖无法修复和未知的安全缺陷、漏洞和后门具有重大意义。

2 基于动态伪装技术的安全防御系统原理

动态伪装技术借鉴了“动态目标防御”的理念,在我国由中国工程院院士邬江兴提出,是在动态防御的基础上发展出的新型网络防御理念。采用类似仿生学的概念,借鉴一些动物的习性,模仿动物保护自身或猎捕猎物的方法,来武装网络安全产品。例如,深海中的灯笼鱼,通过模拟亮光来诱捕猎物;如变色龙,通过改变自身的颜色来适应环境,隐藏自己[3]。

动态伪装技术是为了防御者在功能等价条件下,提供可控的多样化环境间的主动跳变和动态组合,建立欺骗化、拟态化的高价值、高仿真目标,使攻击者难以察觉和预测目标环境的变化,诱骗攻击者对基于动态伪装技术的安全防御系统进行攻击[4]。同时,使用“漏洞疑阵”技术,不断动态地评估攻击者水平,为其构建独特的攻防环境副本,为其不断地提供适合其水平、适合于目标架构、适合于网络和应用环境的虚假漏洞,使其产生入侵即将成功的错觉,但是入侵总是无法获取实质性进展,使得攻击者陷入漏洞一直能够发现,但是总是无法利用的循环之中,达到掩盖真实漏洞的目的[5]。

3 基于动态伪装技术的安全防御系统设计

动态伪装安全防御模型的基本思想是建立动态仿真系统[6]。

动态仿真系统可以动态模拟真实系统中的任意元素,通过功能等价异构执行体池中异构执行体集构造异构执行体,实现动态伪装。其设计思路如下:

(1)根据动态变换器的计算从异构执行体池中组合出异构执行体,在功能等价异构执行体池中选出若干异构执行体。

(2)当系统输入到达时,由输入分发器分发给各个选出异构执行体,它们分别执行,互相无影响、无通信。

(3)当判断为攻击者对系统进行扫描或者攻击时,输出裁决器将攻击者的输入反馈给拟态变换器,其使用动态调度算法和负反馈控制机制计算选取若干异构构件和执行体组成异构执行体,并将异构执行体进行重构、重组或重建,也可以借助虚拟化技术改变执行体的资源配置或清洗、初始化执行体等,增加虚假漏洞、后门或缺陷数量,造成系统外在特征不确定性的假象,实现隐匿真实系统内未知的漏洞、后门和缺陷的作用[7]。动态伪装防御系统设计如图 1 所示。

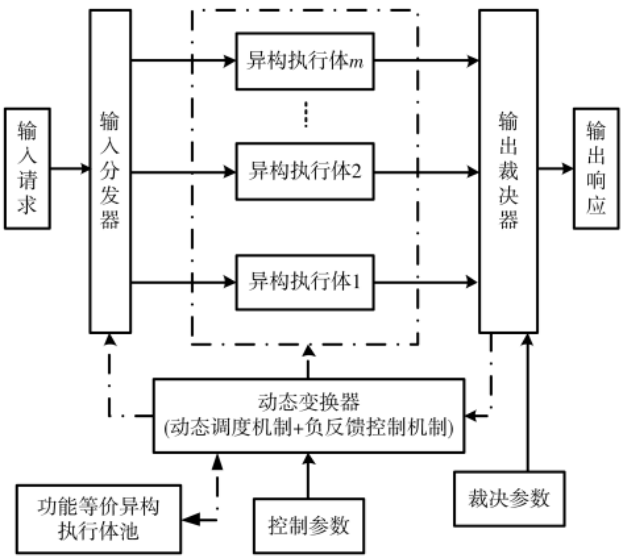

图 1 动态伪装防御系统核心架构图

为了研究方便,不妨假定当前考虑的安全相关基本要素分为 4 层,分别为网络层、计算资源层、软件层、数据层。动态异构执行体变换内容举例如表 1 所示,表中针对假定的 4 种信息系统要素[8],分别列举了要素中对应的基本单元及可变换内容。

设信息系统有 m 个要素,每个要素都有 n 个元素,

表 1 动态异构执行体变换内容举例

信息系统构成要素	基本单元	主要的动态变换内容
网络层	协议	改变目标系统使用的协议
	地址	改变目标信息系统的 IP 地址
	端口	改变目标系统的端口
	----	上述变换多种形式的叠加
计算资源层	操作系统	改变操作系统
	异构冗余设备	异构设备切换
	存储系统	改变存储系统
	虚拟机实例	改变虚拟机实例
	----	上述变换多种形式的叠加
软件层	软件异构变体	软件变体切换
	软件程序的指令序列	改变执行指令序列和形式
	指令格式	动态化存储资源分配方案
	内部数据结构布局	上述变换多种形式的叠加

数据层	数据库管理系统	改变数据库管理系统类型
	数据库	改变数据库结构
	数据	改变数据内容
	----	上述变换多种形式的叠加

$n=\max\{n_1,n_2,\cdots,n_m\}$，$i=1,2,\cdots,m$，其中 n_i 为第 i 个要素的元素个数。对于元素个数少于 n 的要素，以空元素来进行扩充。如果用 x_j^i 表示第 j 个要素中第 i 个元素的状态，那么 t 时刻信息系统的状态可以用矩阵 $\boldsymbol{\Omega}(t)$ 来表示。

$$\boldsymbol{\Omega}(t)=\begin{pmatrix} x_1^1(t),x_1^2(t),\cdots,x_1^n(t) \\ x_2^1(t),x_2^2(t),\cdots,x_2^n(t) \\ \vdots \quad\quad \vdots \\ x_m^1(t),x_m^2(t),\cdots,x_m^n(t) \end{pmatrix} \tag{1}$$

根据拟态安全的思想，动态变换可以定义如下：

$$\sigma:\boldsymbol{\Omega}(t_i)\rightarrow\boldsymbol{\Omega}(t_i+1) \tag{2}$$

设 σ_1 表示第一个要素的动态变换，以此类推，动态异构执行体的要素变换可记为 $\boldsymbol{\sigma}=\{\sigma_1,\sigma_2,\cdots,\sigma_n\}$，则 $\boldsymbol{\sigma}$ 可以看成是 $\boldsymbol{\Omega}(t)$ 的一个加扰序列，不同的加扰序列对应着不同的动态异构执行体变换[9]。

动态变换使得安全防御系统具有不确定性、灵活性、无法预知等特点，改善了传统安全防御系统顺序、固化、静态的防御理念，从而提升了信息系统的整体安全性。

4 基于动态伪装技术的安全防御系统抗网络攻击有效性分析

在进行基于动态伪装技术的安全防御系统抗网络攻击有效性分析前，提出如下假设[10]：

(1)忽略由于硬件错误导致的执行体故障；

(2)暂不考虑分发器和裁决器受到攻击的情况；

(3)攻击者仅基于执行体的漏洞、缺陷和后门发起攻击，不考虑其他非技术手段，而且每次攻击事件是独立的。

本节以图 1 所示的动态伪装系统为研究对象，分别从攻击发起难度、持续攻击难度和攻击再现难度[11]进行分析。

(1)攻击发起难度

①设异构构件集合为 A，$|A|=m$；

②设执行体集合为 B，$|B|=n$。

由随机动态选择算法可知由 A 到 B 有 C_m^n 种可能，设每种可能经裁决器输出后与正常输出不一致的概率为 P_i $(i=1,2,\cdots,)$，因此在该攻击环节攻击成功的概率为：

$$Q=\sum_{i=1}^{C_m^n}P_i \tag{3}$$

由于裁决器本身的特性，P_i 极小，可得 Q 极小。所以，在该环节的攻击成功率极小[12]。

(2)持续攻击难度

攻击者发起一次成功的攻击一般由多个攻击环节组成，缺一步或者错一步都可能造成攻击失败。

设某次成功的攻击行为共涉及 k 个攻击环节，若此次攻击成功，则需 k 个攻击环节都成功。则此次攻击成功的概率为：

$$P=\prod_{x=1}^{k}Q_x \tag{4}$$

此时，$P<<Q$。若在某个环节失败，当攻击者再次尝试一次新的攻击时，由于每个环节的异构构件经过再次的随机动态选择后执行体发生改变，因此相当于发起一次新的攻击。由此可知，在动态安全防御系统中，攻击不具有持续性[13]。

(3)攻击再现难度

设某一次攻击偶然成功，同上分析，当攻击试图再次复现攻击时，由于攻击目标已变，先前的攻击过程并不能复现，因此再次攻击难以成功。

综上所述，基于动态伪装技术的安全防御系统能极大地提升攻击难度、防止攻击再现，是扭转当前“易攻难守”的网络安全现状的必然选择[14]。

5 利用本地代理与云服务模式实现基于动态伪装技术的安全防御系统应用解决方案

通过以上分析，基于动态伪装技术的网络安全防御系统设计思路明确，抗网络攻击有效性相比传统的安全防护系统更高。如何将设计思路与实际信息系统安全防护相结合，是本节讨论的重点内容。

以面向互联网提供服务的 Web 应用为例，将多套不同操作系统、中间件软件、应用软件、数据库管理系统等组成异构体集群部署在云端的 SAAS 服务中。

来自互联网的未知请求数据包通过安全防御系统的本地代理发送给 SAAS 服务平台的分发器，分发器复制多份请求数据包分别发送给各个异构执行体中，在异构执行体中分别处理请求数据包并将响应结果返回给裁决器，裁决器通过预先设计的算法对执行结果进行表决，最终将正常的访问请求返回给本地代理，由本地代理转发正常的访问请求，其经过本地网络设备、安全设备后发送给 Web 应用服务器。如发现疑似攻击行为，将执行结果和非正常请求数据包一同报送威胁溯源分析系统，该系统分析评估攻击者的设备指纹、漏洞扫描、攻击、验证和漏洞利用等行为，持续评估攻击者的水平，结合异构执行体的执行结果，为攻击者制定诱捕策略，构造出具体的虚假漏洞，根据虚假漏洞伪造响应数据包返回给攻击者。为其营造出“攻击还差一步就能成功，但是总也攻不破”的体验，持续吸引攻击者火力，在威胁溯源分析系统中不断对攻击者进行评价，为侦查、反制、预警、预防等动作争取宝贵的处置响应时间。同时，跟踪收集攻击者身份信息，进行身份识别，精准打击。基于动态伪装技术的网络安全防御 SAAS 服务平台架构图如图 2 所示。

6 结论

在当前安全形势严峻的情况下，亟需网络安全创新思路，研究基于动态伪装技术的安全防御系统已成为网络安全领域的重要研究方向[15]。目前，大部分蜜罐易被攻击者识破而被绕过或者自身被攻击而引起更严重的安全问题[16]。因此，本文提出了基于动态伪装技术的网

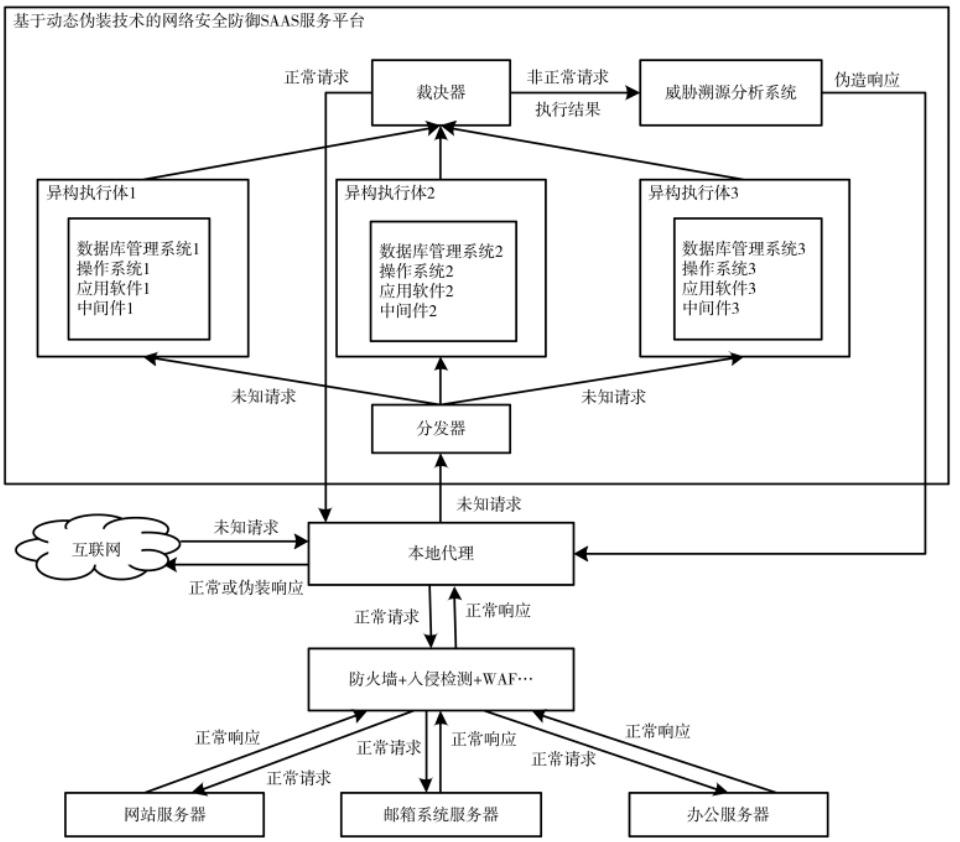

图 2 基于动态伪装技术的网络安全防御 SAAS 服务平台架构图

络安全防御设计理论和应用方案，下一步应将这种安全防御理论运用到物联网、云计算、大数据、移动互联、人工智能、工业控制系统等新技术新应用的网络安全防护之中，提升新技术新应用的整体安全防护水平，以适应新时代安全发展的需求。

参考文献

[1] 冯峰.拟态防御建模与应用层体系结构及安全评估方法研究[D].郑州：郑州大学，2019.
[2] 邬江兴."网络安全再平衡战略"之抓手：拟态防御[J].中国信息安全，2018(6)：46-50.
[3] 申旺强.基于拟态防御的 Web 应用安全技术研究[D].杭州：浙江大学，2016.
[4] 吕志远，陈靓，冯梅，等.拟态防御理论在企业内网安全防护中的应用[J].小型微型计算机系统，2019，40(1)：69-76.
[5] 李政，白利芳，唐刚，等.网络空间安全拟态防御技术概述[J].中国科技纵横，2018(20)：37-39.
[6] 樊永文.基于拟态防御的数据保护安全架构研究[D].郑州：郑州大学，2019.
[7] 梁惠兵.拟态主动防御若干关键技术研究[D].杭州：杭州电子科技大学，2018.
[8] 王硕，王建华，裴庆祺，等.基于动态伪装网络的主动欺骗防御方法[J].通信学报，2020，41(2)：97-111.
[9] 斯雪明，王伟，曾俊杰，等.拟态防御基础理论研究综述[J].中国工程科学，2016，18(6)：62-68.
[10] 胡永进，马骏，郭渊博，等.基于多阶段网络欺骗博弈的主动防御研究[J].通信学报，2020，41(8)：32-42.
[11] 罗婷婷.面向防御的网络欺骗技术研究[J].信息与电脑，2019，31(21)：186-187.
[12] 布日古德.动态网络伪装安全模型研究[D].西安：西北工业大学，2006.
[13] 何永忠，陈美玲.基于协议的拟态研究综述[J].北京交通大学学报，2016，40(5)：1-8.
[14] 常啸林，樊永文，朱维军，等.基于拟态防御的管理信息系统[J].计算机科学，2019，46(z2)：438-441.
[15] 李建军.拟态安全信息系统测评方法及技术研究[J].信息技术与网络安全，2019，38(4)：33-36.
[16] 蔡传晰，梅姝娥，仲伟俊.拟态式蜜罐诱骗机制最优配置策略的博弈分析[J].管理工程学报，2018，32(4)：110-117.

(收稿日期：2021-03-17)

作者简介：
丁朝晖(1977-)，女，硕士，工业互联网安全高级评估师，主要研究方向：网络安全、工控系统安全。
张伟(1976-)，男，硕士，高级工程师，主要研究方向：网络安全、工控系统安全。
杨国玉(1980-)，男，硕士，高级经济师，主要研究方向：信息化与网络安全管理。

扫码下载电子文档

版权声明