DOI 10.15302/J-SSCAE-2016.06.014

# 拟态防御技术

罗兴国[1]，仝青[2]，张铮[2]，邬江兴[1]

（1. 中国人民解放军信息工程大学国家数字交换系统工程技术研究中心，郑州 450002；
2. 中国人民解放军信息工程大学数学工程与先进计算国家重点实验室，郑州 450001）

**摘要：**网络空间安全处于易攻难守的非平衡态势，主动防御技术作为网络空间防御技术的新星，其研究热度不断提高。本文以入侵容忍技术和移动目标防御技术为主线概括了主动防御技术的发展，并介绍了拟态防御技术理论、工程实践以及测试情况。通过分析对比拟态防御和入侵容忍、移动目标的异同，提出网络安全再平衡战略的研究重点和方向，为国家网络空间安全发展提供借鉴和参考。

**关键词：**拟态防御；主动防御技术；网络安全再平衡
**中图分类号：**TN915　　**文献标识码：**A

# Mimic Defense Technology

**Luo Xingguo[1], Tong Qing[2], Zhang Zheng[2], Wu Jiangxing[1]**

(1. National Digital Switching System Engineering & Technological R&D Center, The PLA Information Engineering University, Zhengzhou 450002, China; 2. State Key Laboratory of Mathematical Engineering and Advanced Computing, The PLA Information Engineering University, Zhengzhou 450001, China)

**Abstract:** Cybersecurity is in an unbalanced situation: It is easy to attack cybersecurity but difficult to defend it. Active defense technology is a new direction in cybersecurity research that has attracted more and more attention. This paper summarizes the development of active defense via the introduction of intrusion tolerance technology and moving target defense technology. We then introduce the theory, implementation, and testing of mimic defense. By comparing mimic defense with intrusion tolerance and moving target defense, we propose a research direction and a key point in the cybersecurity rebalancing strategy in order to provide a reference for the development of national cybersecurity.

**Key words:** mimic defense; active defense technology; cybersecurity rebalance

## 一、网络空间安全态势

随着社会信息化和全球网络化进程的推进，国家安全和政治、经济、社会发展对网络空间的依赖程度日益加剧，使得网络空间成为当今社会功能和社会活动的重要支撑。然而，网络空间的广泛脆弱性使世界各国都面临着前所未有的国家安全威胁形势。网络犯罪、网络恐怖主义、黑客攻击以及网络战对国家安全的威胁凸显，迫使各国将网络空间安全提升至国家安全的战略高度，强调网络空间对于国家利益和国家安全具有非常重要的地位和意义，开始将网络空间视为陆、海、空、天之后的“第五空间”。

目前，网络空间攻防态势基本上处于“易攻难

**收稿日期：**2016-10-10；**修回日期：**2016-10-25
**作者简介：**罗兴国，中国人民解放军信息工程大学国家数字交换系统工程技术研究中心，教授，博士生导师，主要研究领域为信息通信网络、网络安全；E-mail: lxg@ndsc.com.cn
**基金项目：**中国工程院重大咨询项目“网络空间安全战略研究”(2015-ZD-10)
**本刊网址：**www.enginsci.cn

守”状态，这就造成了攻击和防御在诸多方面的不对称。网络空间信息系统在设计链、生产链、供应链及服务链等环节存在可信度或安全风险不受控的情形，使得任何国家或组织都无法从根本上消除信息系统或网络基础设施的安全漏洞，而攻击者只需发现并成功利用其中的一个漏洞，就可能给系统带来难以预估的安全风险。

尽管大部分防御技术与防御产品，如防火墙、防病毒软件、基于特征的入侵检测技术等得到了广泛使用，然而这些技术是以阻挡和检测为主要手段，具有一定的被动性和滞后性[1]，属于静态的被动防御方法，尤其难以很好地应对未知漏洞和后门的威胁，存在防御缺陷。

在被动防御技术难以应对未知漏洞、后门问题的困境下，主动防御技术逐步发展并成为研究的焦点。主动防御是指能够在攻击的具体方法和步骤被防御者知悉之前实现防御部署，有效抵抗未知攻击的破坏的防御技术。相对于被动防御技术，主动防御能够降低攻击对系统的破坏性，最大程度防范攻击的发生或进行，尤其是针对未知的攻击，能够实施更加主动的、前摄的防御。典型的主动防御技术，有入侵容忍、移动目标、拟态防御等。其中拟态防御作为我国新兴的主动防御技术，其优势在工程实践与应用中得到了较好的实现和验证，在网络空间安全防御中具有可观的发展前景，有望成为“网络空间再平衡战略”的有力抓手。

## 二、主动防御发展历程

网络空间主动防御技术是相对于传统防御技术提出的，强调系统在受到攻击前能够主动发现、应对随时可能发生的攻击。传统的防御手段如入侵检测、病毒检测、防火墙等方法往往是在攻击发生以后，通过分析攻击行为特征、病毒代码等提出针对性的防御措施，并辅以沙箱、蜜罐等手段捕捉攻击行为，通过打补丁、软件升级等方式试图减少软硬件漏洞[2]。然而这些手段难以从根本上消除漏洞，也不能很好地应对未知漏洞和后门的威胁，属于滞后的防御手段。主动防御技术目标通常是构造安全的系统架构或运行方式，尽可能从根本上增大攻击的难度，降低攻击成功的概率，对广义上的攻击行为进行有效的遏制，从而实现系统的安全。因而，主动防御技术在新型的、未知的攻击行为面前具有较强的抵抗性，是网络安全领域的研究热点之一。

主动防御技术的早期形态以入侵容忍技术为主。入侵容忍技术是由容错技术发展而来的。容错技术最初针对的是计算机系统尤其是分布式系统的计算结果一致性问题而提出的。20 世纪 80 年代，容错技术开始应用于恶意漏洞的防御，由“容错”发展为“容侵”，由此产生“入侵容忍”的概念[3]。入侵容忍借用容错技术来达到容侵、保持系统可生存性和弹性的目的，是当时主流的信息系统安全技术之一。基于入侵容忍技术产生的系统被称作入侵容忍系统（ITS）。入侵容忍系统没有明确的和广泛采用的定义，但可概括为：即使在面临部分组件被成功攻击时，仍然可以持续正确地工作且向用户提供预期的服务的系统[4~7]。

入侵容忍系统的实现基本分为三种类型：检测触发型、算法驱动型和混合型。检测触发型的入侵容忍系统主要通过入侵检测发现入侵行为，继而触发系统的恢复操作以清除入侵，达到入侵容忍的目的。算法驱动型的入侵容忍系统多通过大数表决及其衍生算法和拜占庭表决算法掩盖部分组件的失效或故障。也存在两种类型混合的入侵容忍系统，如 SITAR，既进行表决，也对系统的内部错误进行检测。

入侵容忍的共同目标是保证系统的可用性和弹性，即当系统受到破坏时能够继续维持正常服务或在最短时间内切换服务器使服务持续，尽可能减少平均故障时间。由于入侵容忍技术在主动防御概念之前出现，在防御思路上已经具备了主动防御的特点，同时受限于当时网络威胁的特点，在入侵容忍系统的设计思路上具有一定的局限性，而入侵容忍的提出和丰富的设计方案为主动防御技术的发展提供了研究起点和基础。

由于冗余代价较高，入侵容忍技术研究在维持了 20 年左右的时间后，逐渐没落。为破解网络防御困局，以美国为首的部分国家积极转变防御理念，以主动防范未知漏洞或威胁为目标，以大幅度增加网络攻击风险和代价为手段，着力增强网络防御的灵活适应性与动态自主性，大力探索主动防御新技术，以理论和技术的革命性创新确保美国在网络攻防领域的压倒性优势，并制定了一系列的战略规划、计划和纲领性文件，开展顶层设计。移动

目标防御技术应运而生，2011 年美国科学技术委员会发布了《可信网络空间：联邦网络空间安全研发战略规划》，将“移动目标防御（MTD）”确定为“改变游戏规则”的革命性防御技术[8]，并制定了由联邦政府、产业和学术机构共同参与的网络安全研发框架，保障研发规划的落实。

在美国的带动和刺激下，俄、英、法、印、日、德、韩等国纷纷跟进，将网络空间安全提升至国家战略层面，全面推进相关制度创设、力量创建和技术创新，试图在塑造全球网络空间新格局进程中抢占有利位置。以“主动变化、增加攻击者攻击难度”为典型特征的主动防御技术成为了网络防御技术发展方向。

移动目标防御旨在设计能够在非安全环境中可靠工作的弹性系统，其技术愿景是在多个不同的系统维度上，开发、分析和部署防御者可控的、随时间动态迁移和变化的机制和策略，以限制自身脆弱性的暴露，降低被攻击的机会，同时大幅增加攻击者的成本[9]。移动目标防御技术在网络层、平台层、运行环境、软件层和数据层都具有应用场景，共同的特点是通过动态地改变系统的配置、组成或状态，使系统具有动态性、随机性、难以预测性，从而使攻击者难以发现攻击目标，或难以针对目标的漏洞实施有效的攻击。

移动目标防御改变了长久以来的静态设计，提出增加动态性以提高安全性，是主动防御的重要理念之一。移动目标防御技术的提出在很大程度上提升了主动防御技术的研究热度。

## 三、拟态防御理论与实践

近年来，伴随着多起震惊世界的网络安全事件的曝光，全球各国对网络空间安全的重视程度不断提高。在国家级网络空间安全战略的引领下，拟态防御针对网络空间未知漏洞和后门问题，提出采用“有毒带菌”组件和“沙滩建楼”方法构建由内生防御机理保证的风险可控、安全可信的系统[2]。

拟态防御技术以功能等价条件下的变结构拟态计算为基础，以高可靠的非相似余度“容错”模式为基本架构，以非配合条件下的多模裁决为核心机制，并以在装置的服务功能与其外在的结构表征之间导入不确定性关系为重点，利用动态异构冗余构造的控制调度管理环节引入复合调度策略，利用动态异构冗余构造的可重构、可重组、可重建、可重定义和虚拟化等构造方法，增强功能等价条件下装置结构表征的不确定性并扰乱攻击者的信息链，使攻击者探测感知或预测防御行为与特征的难度呈非线性增加，使攻击成果的有效利用转化为极小概率事件。

目前，拟态防御技术已在路由器和 web 服务器上进行了原理实践和验证，相关的产品化工作和其他原理验证研究也在同步开展中。

2016 年 1 月至 6 月，受国家科技部委托，上海市科委组织国家信息技术安全研究中心等 9 家权威检测单位，组成联合测试团队对拟态防御原理验证系统开展了测试验证工作。

测评对象为两种应用场下的拟态防御原理验证系统，一种是属于信息通信网络基础设施范畴的拟态路由器或交换机原理验证系统，另一种是属于网络信息服务范畴的拟态 web 服务器原理验证系统。为了检验拟态系统的内生防御机理，测试程序规定评测对象不得安装任何防护工具，测试过程中不能进行任何形式的漏洞修补或后门封堵等增量开发，也不能使用诸如防护墙、加密认证等安全手段。

测试采取了包括使用黑盒测试、白盒测试、渗透测试、对比测试等在内的多种测试方法和手段，也包括预置后门和配合注入病毒木马等方式，测试验证以下五个方面的问题。

（1）拟态防御系统能否隐匿拟态界内的未知漏洞和后门。

（2）攻击方能否利用拟态界内未知漏洞注入未知病毒木马。

（3）防御方能否有效抑制拟态界内基于未知因素的协同攻击。

（4）能否允许拟态界内使用“不可信、不可控”的软硬构件。

（5）拟态界内运行环境能否允许“有毒带菌”。

测试中共完成了 13 类、113 项、204 例验证测试。所有测试验证都是在保证目标对象服务功能和性能前提下进行的，验证测试结果与理论预期完全吻合。测试结果和分析评估结果表明受测系统是拟态防御理论与方法的成功实践，同时也验证了拟态防御原理的正确性和可行性，进一步说明应用系统工程思想能够在理论和实践上解决

网络空间安全防御的难题。

拟态防御是一种内生的安全架构技术，对架构内的未知漏洞、陷门、后门甚至一些未知的病毒和木马具有自然免疫力，与现有的被动防御手段的有效融合可以形成对抗网络空间已知或未知攻击的能力。但拟态防御并不企图一劳永逸地解决网络空间的所有安全问题，也不奢望独立地构建任何安全防护体系，不排除融合已被证明具有安全效果的任何防御体系和技术手段，更不阻碍接纳未来可能出现的新安全技术或方法。总之，拟态防御对现有网络空间安全防御体制具有互补性，在技术上具有融合性，在产品上具有自主可控性。

## 四、主动防御优势与挑战

拟态防御、入侵容忍和移动目标同属于主动防御技术范畴，而这三种技术在提出背景、实现方法、技术愿景等方面不尽相同。

入侵容忍以维持系统可用性为主要目的，使系统具有较强的生存能力和恢复能力，从而减少平均故障时间，提高系统可生存性，保证了服务、数据等的可靠性。然而入侵容忍对于性价比的研究和探索较少，直观上看，冗余和表决将带来较高的资源成本和时延，因而性价比问题可能是导致入侵容忍技术没落的主要原因。

移动目标防御能够提高攻击门槛，对攻击目标起到一定的隐蔽作用。由于攻击行为一般具有较强的针对性，因而，通过动态变化使系统静态性减弱，能够使攻击者难以定位攻击目标，从而起到一定的隐蔽作用，增大了攻击发起的难度。然而，要保持动态性和有效的防御，需要系统具有较高的变化频率，可能会对系统的性能造成一定的损失，性能和变化频率的折衷将是移动目标防御研究的重点之一。另一方面，多样呈现的系统在特定时刻下仍是单一性质的系统，可能会给攻击者提供更大的攻击面和更多的攻击目标，对系统的防御起到反作用。

拟态防御能够扰乱攻击者与被攻击对象的信息链，扰乱攻击者的判断，从而造成攻击发起难、持续难、再现难。拟态防御既能够维持可用性，同时也能够对被攻击目标起到隐蔽作用。与移动目标的隐蔽原理不同，拟态防御通过表决输出的方式“中和”或掩盖被攻击目标的输出，从而对外表现为无异常或攻击无效，扰乱攻击者对攻击成败和效果的判断。相比入侵容忍技术，拟态防御在防御目的上更倾向于对安全性整体的防护而不仅仅是可用性。拟态防御的技术组合具有调优的潜力，能够用相对较少的资源开销实现相对较高的防御能力，具有较好的发展前景。

入侵容忍和移动目标防御技术的研究和应用集中在以美国为主的发达国家，在这两项主动防御技术的研究中，我国虽然加紧跟进，却始终处于滞后地位。拟态防御作为我国自主提出的网络空间主动防御技术，在网络空间安全的重要性不断被提升的形势下，需把握先机，加快推进，打造我国自主可控的防御策略体系，构建主动防御堡垒，打破网络安全在攻防博弈、大国博弈的不平衡态势，为重构我国网络空间安全地位提供支撑。

## 五、网络安全再平衡战略

拟态防御技术作为我国新兴的主动防御技术，能够在“软硬构件供应链不可控、不可信”的前提下，支撑全球化时代网络安全与信息化“一体两翼，双轮驱动”发展目标的实现，有助于消除网络安全与信息化融合领域给全球自由贸易造成的有形或无形壁垒，使得基于未知漏洞、后门、病毒木马等攻击失去威胁和震慑作用，显著增加攻击代价，创造网络信息领域新需求，促进功能等价异构多元化市场的繁荣，同时不再只是排他性竞争。拟态防御为国家级信息系统自主可控发展战略提供了一条新思路。需要综合利用国家资源优势，加快推进拟态防御应用推广，为网络安全再平衡战略提供有力抓手。

### （一）应用推广

在拟态防御前期原理验证系统的研制和测试基础上，进一步研制拟态路由器或交换机、拟态 web 服务器、拟态文件或数据存储系统、拟态防火墙或网关等可产品化的软硬件技术成果。

作为战略性任务，需动员全社会力量发展完善拟态防御相关理论与方法，进一步提炼优化关键技术，推进技术的创新与融合，为拟态防御的产品化、定制化发展提供完备的理论体系和技术体系保障。

拟态防御作为普适性原理和方法，应发动相关

行业技术力量结合本领域特点，研究定制化的实现技术，开展拟态防御产品试验示范应用，推动拟态防御产品在各行业领域的应用，促进拟态防御技术的产业化。

### （二）标准制定

拟态防御研究团队有责任、有义务以拟态防御技术为出发点，制定出拟态防御技术乃至主动防御技术相关的指标体系和测试规范，编制完成满足拟态防御设备或系统认证评估要求的分级指标体系，形成国家标准和行业规范，为拟态防御技术的完善和主动防御技术的发展添砖加瓦。

### （三）政策策略

在政策与策略研究上，应着力发挥技术领跑优势，快速抢占产业和市场先机，尽快形成网络空间新型防御能力，为网络安全与信息化融合领域释放出“网络安全再平衡战略”所需的创新活力与动力。

#### 参考文献


[1] Kenkre P S, Pai A, Colaco L. Real time intrusion detection and prevention system[C] //Satapathy S C, Biswal B N, Udgata S K, et al. Proceedings of the 3rd international conference on frontiers of intelligent computing: Theory and applications (FICTA)2014. Switzerland: Springer International Publishing, 2015 (1): 405–411.

[2] Wu J X. Mimic security defense in cyber space [J]. Secrecy Science and Technology, 2014, 10(1): 4–9.

[3] Powell D, Stroud R. Project IST-1999-11583 malicious- and accidental-fault tolerance for internet applications: Conceptual model and architecture of MAFTIA [R]. Newcastle: University of Newcastle upon Tyne, 2003.

[4] Jajodia S, Ghosh A K, Swarup V, et al. Moving target defense: Creating asymmetric uncertainty for cyber threats [M]. New York: Springer, 2011.

[5] Gupta V, Lam V, Ramasamy HG V, et al. Dependability and performance evaluation of intrusion-tolerant server architectures [M]. Berlin: Springer, 2003.

[6] Wang F, Jou F, Gong F, et al. SITAR: A scalable intrusion-tolerant architecture for distributed services [C]// Proceedings of the 2001 IEEE— Workshop on information assurance and security. New York: United States Military Academy, 2003.

[7] Malkhi D, Reiter M. Byzantine quorum systems [J]. Distributed Computing, 1998, 11(4): 203–213.

[8] Kewley D L, Bouchard J F. DARPA information assurance program dynamic defense experiment summary [J]. IEEE Transactions on Systems, Man, and Cybernetics. Part A, Systems and Humans, 2001, 31(4): 331–336.

[9] Okhravi H, Hobson T, Bigelow D, et al. Finding focus in the blur of moving-target techniques [J]. IEEE Security & Privacy, 2014, 12(2): 16–26.