基于模糊控制的虚拟服务器暴露时间的确定

秦振翔，马润年
（空军工程大学信息与导航学院，西安，710077）

摘要 针对动态防御平台中的服务器最大可暴露时间难以确定的问题，利用模糊控制相关理论与技术，设计了可以确定虚拟服务器最大可暴露时间的模糊控制器，在保证系统安全的前提下，实现跳变引起的防御成本最小化。假设防御者清楚状态攻击面，且攻击者不能在某个时间段内完成攻破。首先从平台层移动目标防御原理入手，计量出系统攻击面的数学期望，再对各虚拟服务器的系统漏洞进行定量分析，并将此2个指标作为模糊控制器的输入，在保证系统安全的状况下，最后计算虚拟服务器的最大可暴露时间，为切换虚拟服务器过程中确定时间点提供了重要的参考依据。

关键词 虚拟服务器；攻击面数学期望；系统漏洞评估；模糊控制器；最大暴露时间
DOI 10.3969/j.issn.1009-3516.2020.05.012
中图分类号 TP393.08；TN918 **文献标志码** A **文章编号** 1009-3516(2020)05-0076-06

Determination of Virtual Server Exposure Time Based on Fuzzy Control

QIN Zhenxiang, MA Runnian
(Information and Navigation College, Air Force Engineering University, Xi'an 710077, China)

Abstract Aimed at the problem that the maximum exposure time of the server in the dynamic defense platform is hard to determine, this paper utilizes the fuzzy control-related theories and technologies for designing a fuzzy controller, determining the maximum exposure time of the virtual server and minimizing defense costs due to change. Thepaper assumes that the defender knows the attack surface and the attacker cannot complete the attack within a certain period of time. Firstly, Starting from the platform-level moving target defense principle, the mathematical expectation of the system attack surface is measured. Secondly, the system vulnerability of each virtual server is quantitatively analyzed, and these two indicators are used as inputs to the fuzzy controller to ensure the security of the system. Finally, the maximum exposure time of the virtual server is calculated, providing an important reference for determining the time point during the virtual server switching process.

Key words virtual server; attack surface mathematical expectation; system vulnerability assessment; fuzzy controller; maximum exposure time

近些年来，先进可持续性威胁(Advanced Persistent Threat，APT)的发展使网络安全的形势越来越严峻。传统防御网络所特有的确定性、相似性、静态性及漏洞的持续性是现有网络信息系统的致命

收稿日期：2019-11-24
基金项目：国家自然科学基金(61573017)
作者简介：秦振翔(1996—)，男，安徽合肥人，硕士生，主要从事网络空间安全理论研究。E-mail:18855495269@163.com

引用格式：秦振翔，马润年. 基于模糊控制的虚拟服务器暴露时间的确定[J]. 空军工程大学学报(自然科学版)，2020，21(5)：76-81. QIN Zhenxiang, MA Runnian. A Determination of Virtual Server Exposure Time Based on Fuzzy Control[J]. Journal of Air Force Engineering University (Natural Science Edition), 2020, 21(5): 76-81.

安全缺陷[1]。这些缺陷将直接导致网络信息系统始终处于被动挨打的局面。因此，完善防卫系统的防御强度就十分必要。然而，无论防御强度有多高，只要主机处于静止状态，攻击者总有办法通过时间成本来换取攻击效益。移动目标防御就是设法打破这种静止状态，从而可以增加攻击成本，使攻击者得不偿失。目前，在对移动目标防御中软件层、平台层、网络层和数据层进行的相关研究中，前人已取得了不少成果。

平台层的移动目标防御通过构建多样化的运行平台，进而动态改变其运行环境，缩短应用在某平台上的暴露时间。文献[3]应用了相关 Web 服务多样化技术，提出了虚拟服务器软件栈的设计方案，却未进一步对虚拟服务器的最大可暴露时间做定量分析；文献[4]利用多样化的软件栈模板，设计了基于异构平台的虚拟服务器池，未对虚拟服务器的最大可暴露时间进行定量分析；文献[5]在平台暴露时间和随机迁移次序等因素影响下，提出了 3 种面向隔离区的主动迁移策略，未进一步对迁移时间做定量分析；文献[6]基于前人移动目标防御的研究成果，进行了分类与总结，不需要定量分析虚拟服务器的最大可暴露时间；文献[7]对动态平台技术作为防御机制进行了定量评估，没有进一步分析虚拟服务器的最大可暴露时间；文献[8]基于云计算对 Web 防御系统进行了相关的研究，不需要对虚拟服务器的最大可暴露时间进行定量分析；文献[9]针对传统 Web 服务可信性难以适应动态评估的问题，提出了一种基于信息熵权重和带修正指标的动态信任评估模型（Dynamic Trustworthy Evaluation based on Information Entropy and Correction Metrics，DTEIECM），不需要对虚拟服务器的最大可暴露时间进行定量分析；文献[10]针对传统网络的静态等特性，提出了一种软件定义 APT 攻击移动防御网络架构（Software Defined Moving Target Defense Architecture，SDMTDA），不需要对虚拟服务器的最大可暴露时间进行定量分析；文献[11]针对端信息跳变的有关问题，提出了一种基于非广延熵和 Sibson 熵融合的实时网络异常度量算法，不需要对虚拟服务器的最大可暴露时间进行定量分析。而这些都未定量地对防御平台中虚拟服务器的最大可暴露时间进行分析。

不同的虚拟服务器在平台上的暴露时间会有所不同，可能是因为各服务器中的被攻击面不同。目前，很少有文献在保证系统不被攻破的前提下对服务器的最大可暴露时间进行定量的研究。本文假设防御者清楚状态攻击面，且攻击者不能在某个时间段内攻破。那么，保证系统虚拟服务器安全的时间至少大于系统虚拟服务器的最大可暴露时间。因此本文试图基于模糊控制相关理论与技术，以攻击面的度量结果和漏洞评估结果为输入，最终输出服务器的最大可暴露时间，达到保证系统虚拟服务器不被攻破的目的。

1　模型描述

如图 1，基于模糊控制技术，对受到攻击的虚拟服务器进行相关攻击信息的采集，分析后得到攻击面数学期望，再根据国家信息安全漏洞库（China National Vulnerability Database of Information Security，CNNVD）中的漏洞分级规范对系统漏洞进行评估，得到一个评估分数，再将这 2 个指标输入到模糊控制器中，得到该服务器最大暴露时间。再将暴露时间反馈到控制程序，作为确定切换到下一个服务器时间点的参考依据。

虚拟服务器一般由 4 个部分组成，每一个部分都有具体的构成形式，Web 服务多样化即是让各部分的具体构成形式在兼容模式下进行任意组合。

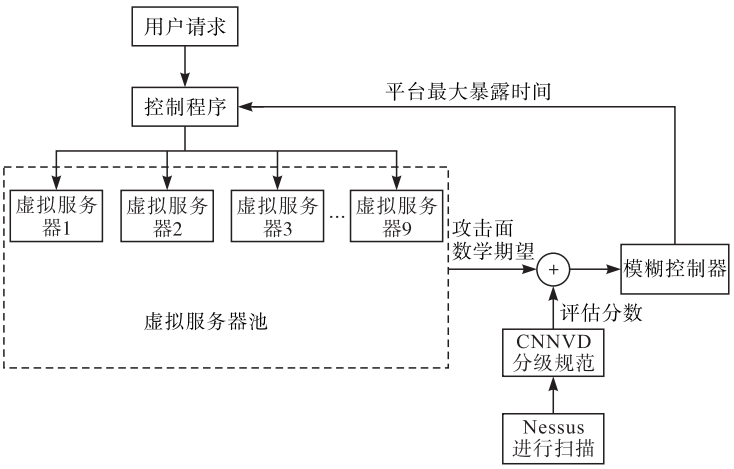

图 1　基于模糊控制确定平台暴露时间体系结构

1.1 攻击面定量分析

攻击面是攻击者进入被攻击系统的“桥梁”。一般来说,攻击者可以通过一些系统的内部程序、系统通道(如套接字)等和系统中共享的数据项来对目标系统发起攻击。这些资源在系统中某一时刻存在的可被攻击点统称为攻击面[11]。在此,可以用 Nessus 对 Web 虚拟服务器进行漏洞扫描,将漏洞作为攻击面。

为了方便研究,设定 9 个虚拟服务器。每个虚拟服务器均有 3 种模式,即在线模式、关闭模式和离线模式。在线模式下,接受攻击并收集攻击者信息;关闭模式下,将收集到的攻击信息进行分析;离线模式下,对存储的攻击信息进行清零操作,为再次收集做好准备。

设 A_i 表示虚拟服务器 i 的在线模式,$i=1,2,\cdots,9$。假定 9 个虚拟服务器只有一个处于在线模式,并且假设在平稳状态下虚拟服务器 i 处于在线模式的概率为 x_i,各个虚拟服务器的模式切换符合马尔科夫链。规定服务器在完成切换的同时,在线模式会自动转变成关闭模式,最后变成离线模式。设状态 A_i 转移到状态 A_j 的转移概率(各虚拟服务器间的切换概率)为 p_{ij},可得此系统状态转移矩阵为:

$$\boldsymbol{p}=\begin{bmatrix} p_{11} & \cdots & p_{1n} \\ \vdots & & \vdots \\ p_{n1} & \cdots & p_{nn} \end{bmatrix} \tag{1}$$

设各个状态间转移时间的间隔相等均为 $\Delta t\in[0,1]$,随机化程度 $R\in[0,1]$,防御者对攻击者探测报文的拦截率 $t\in[0,1]$,p_{di} 是攻击者探测到漏洞的概率,满足以下函数关系:

$$p_{di}=\frac{\Delta t}{T_0}\times R\times L$$

式中:T_0 表示为扫描到该虚拟服务器中所有攻击面(在此指漏洞)所需时间的最大值。

本文假设防御者清楚状态攻击面,且攻击者不能在某个时间段内攻破。在状态空间 $A=\{A_1,A_2,\cdots,A_9\}$ 中,我们任意设定其中的状态转移(服务器切换)规则为:若转移前它在 $A_2,A_3,\cdots,A_8$,则它分别以 1/3 的概率向前、向后转移或者保留原处;若转移前,它在 A_1,则它以概率 1 转移到 A_2;若转移前,它在 A_9,则它以概率 1 转移到 A_8。由此可得此系统的状态转移(服务器切换)概率矩阵为:

$$\boldsymbol{p}=\begin{bmatrix} 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ \frac{1}{3} & \frac{1}{3} & \frac{1}{3} & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & \frac{1}{3} & \frac{1}{3} & \frac{1}{3} & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & \frac{1}{3} & \frac{1}{3} & \frac{1}{3} & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & \frac{1}{3} & \frac{1}{3} & \frac{1}{3} & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & \frac{1}{3} & \frac{1}{3} & \frac{1}{3} & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & \frac{1}{3} & \frac{1}{3} & \frac{1}{3} & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & \frac{1}{3} & \frac{1}{3} & \frac{1}{3} \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{bmatrix} \tag{2}$$

由马尔科夫链的相关基础知识可得:平稳状态 $X=(x_1,x_2,\cdots,x_9)$ 可根据 $X=X\boldsymbol{p}$ 可得:

$$\begin{cases} x_1=\frac{1}{3}x_2 \\ x_2=x_1+\frac{1}{3}x_2+\frac{1}{3}x_3 \\ x_3=\frac{1}{3}x_2+\frac{1}{3}x_3+\frac{1}{3}x_4 \\ x_4=\frac{1}{3}x_3+\frac{1}{3}x_4+\frac{1}{3}x_5 \\ x_5=\frac{1}{3}x_4+\frac{1}{3}x_5+\frac{1}{3}x_6 \\ x_6=\frac{1}{3}x_5+\frac{1}{3}x_6+\frac{1}{3}x_7 \\ x_7=\frac{1}{3}x_6+\frac{1}{3}x_7+\frac{1}{3}x_8 \\ x_8=\frac{1}{3}x_7+\frac{1}{3}x_8+\frac{1}{3}x_9 \\ x_9=\frac{1}{3}x_8 \\ x_1+x_2+\cdots+x_9=1 \end{cases} \tag{3}$$

解得:$X=(1/23,\ 3/23,3/23,3/23,3/23,3/23,3/23,3/23,1/23)$

不管初始状态什么样,系统在经过转移后,达到一个马尔科夫平衡状态。据此,可算出攻击面的数学期望值:

$$\overline{E}=x_1k_1p_{d1}+x_2k_2p_{d2}+\cdots+x_9k_9p_{d9} \tag{4}$$

式中:k_i 表示第 i 个虚拟服务器中的可被攻击点的个数,在此为 Nessus 扫描到的漏洞个数。

根据此前假设,防御者是熟悉状态攻击面的,那么防御者便会刻意引导系统往攻击面小的方向进行转移。假设初始状态下的攻击面为 $k_1=7$,$k_2=3$,$k_3=5$,$k_4=1$,$k_5=6$,$k_6=8$,$k_7=4$,$k_8=2$,$k_9=9$,攻击面探测概率 $p_{d1}=0.4$,$p_{d2}=0.6$,$p_{d3}=0.5$,$p_{d4}=$

0.7，$p_{d5}=0.45$，$p_{d6}=0.35$，$p_{d7}=0.55$，$p_{d8}=0.3$，$p_{d9}=0.6$，根据$\overline{E}$的计算公式可得到攻击面的数学期望$\overline{E}=2.09$。

1.2　操作系统漏洞评估

本文基于 CNNVD 漏洞分级规范来对 Nessus 扫描到的线上虚拟服务器的漏洞进行相关评估。凡是被 CNNVD 收录的漏洞，均适用此分级规范，包括采集的公开漏洞以及收录的未公开漏洞，通用型漏洞及事件型漏洞[14]。该项评估主要基于可利用性指标组和影响性指标组来对其进行定量评估。

如表 1、表 2 所示，根据以下 7 种指标来对系统漏洞进行评估，再根据 CNNVD 分级规范给定的评分表，即可得出 2 组指标的评分。2 组指标的评分和为评估结果。如：攻击途径为网络、攻击复杂度低、无权限要求和不需要用户交互的情况下，可用性指标组评分为 3.89；在高机密性影响、高完整性影响和高可用性影响的情况下，影响性指标组评分为 5.87。因此 2 组评分和 9.76 即为最终的评分结果。

表 1　可攻击性指标

要素	符号	可选值
攻击途径	Access Vector	网络/邻接/本地/物理
攻击复杂度	Access Complexity	高/低
权限要求	Privilege	高/低/无
用户交互	Interaction	需要/不需要

表 2　影响性指标

要素	符号	可选值
机密性影响	ConfImpact	高/低/无
完整性影响	InterImpact	高/低/无
可用性影响	AvailImpact	高/低/无

2　模糊控制系统

在目前的平台层的移动目标防御研究中，很少有对服务器最大可暴露时间做出相关定量研究。因此，本文试图运用模糊控制系统在仿真环境中对服务器可暴露时间做出定量分析。

本文将攻击面数学期望 $\overline{E}$ 和系统漏洞评估分数 S 这 2 个指标，作为模糊控制器的 2 个输入变量，结合模糊控制的思想，得到虚拟服务器可暴露时间 τ，再根据这一重要指标来确定切换虚拟服务器的时刻，最终以获得最大防御收益。模糊控制具体框图见图 2。

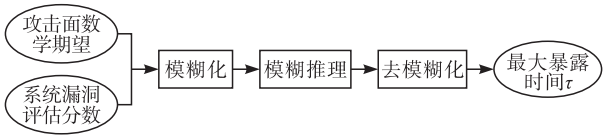

图 2　模糊控制原理框图

2.1　模糊化

在模糊控制系统中，为方便研究，将 2 个输入量分别模糊化成 3 个子集、输出量模糊化成 5 个子集，再选取三角形隶属函数。

1）对于攻击面数学期望，选定 3 个模糊子集：期望值小（E_S）、期望值中（E_M）、期望值大（E_L）。为研究方便，假设输入 x 的定义域为[0,6]，则可得其隶属函数：

$$E_S(x)=\frac{3-x}{3},0\leqslant x\leqslant 3$$

$$E_M(x)=\begin{cases}\dfrac{x}{3},0\leqslant x\leqslant 3\\ \dfrac{6-x}{3},3<x\leqslant 6\end{cases}\tag{5}$$

$$E_L(x)=\frac{x-3}{3},3<x\leqslant 6$$

2）对于系统漏洞评估分数，选定 3 个模糊子集：分数低（S_S）、分数中（S_M）、分数高（S_L）。根据 CNNVD 的分级标准，可得评估分数在[0,10]内，大于 10 的以 10 来代替。因此，输入 y 的定义域为[0,10]，则可得其隶属函数：

$$S_S(y)=\frac{5-y}{5},0\leqslant y\leqslant 5$$

$$S_M(y)=\begin{cases}\dfrac{y}{5},0\leqslant y\leqslant 5\\ \dfrac{10-y}{5},5<y\leqslant 10\end{cases}\tag{6}$$

$$S_L(y)=\frac{y-5}{5},5<y\leqslant 10$$

3）对于输出量即服务器可暴露时间，选定 5 个模糊子集：很短（S_V）、短（S）、中等（M）、长（L）、很长（L_V）。为研究方便，假设输出 τ 的值域为[0,12]，以 min 为时间单位，可得其隶属函数如下：

$$S_V(\tau)=\frac{2-\tau}{2},0\leqslant\tau\leqslant 2$$

$$S(\tau)=\begin{cases}\dfrac{\tau}{2},0\leqslant\tau\leqslant 2\\ \dfrac{5-\tau}{3},2<\tau\leqslant 5\end{cases}$$

$$M(\tau)=\begin{cases}\dfrac{\tau-2}{3},2\leqslant\tau\leqslant 5\\ \dfrac{8-\tau}{3},5<\tau\leqslant 8\end{cases}\tag{7}$$

$$L(\tau)=\begin{cases}\dfrac{\tau-5}{3},5\leqslant\tau\leqslant 8\\ \dfrac{12-\tau}{3},8<\tau\leqslant 12\end{cases}$$

$$L_V(\tau)=\frac{\tau-8}{4},8<\tau\leqslant 12$$

2.2 模糊推理

根据已有的攻防先验知识,系统越危险,在保证系统不被攻破的前提下,虚拟服务器完成切换越快,其暴露时间就会越短。因此,切换要尽快完成。据此有以下模糊规则:

1)攻击面数学期望越大,漏洞评估分数越高,服务器可暴露时间就越短;

2)攻击面数学期望适中,漏洞评估分数适中,服务器可暴露时间就适中;

3)攻击面数学期望越小,漏洞评估分数越低,服务器可暴露时间就越长。

在此,假设漏洞评估分数对服务器可暴露时间影响更大且更显著。对攻击面数学期望和漏洞评估分数各 3 种情况进行组合,可得到具体的模糊规则,见表 3。

表 3 模糊控制的具体规则表

暴露时间 t / 期望 x \ 分数 y	S_L	S_M	S_S
E_L	$S_V(1)$	$M(4)$	$L(7)$
E_M	$S(2)$	$M(5)$	$L(8)$
E_S	$M(3)$	$L(6)$	$L_V(9)$

注:暴露时间后的(1)、(2)、…、(9)按时间长短排列的序号。

2.3 去模糊化

根据以上的模糊规则,在理想状态下,总的集合应由上述所有的规则进行并集运算得到。然而在一般情况下,由于每次的输入量不可能全部激活上述规则,因此根据这一特点,只取出激活了的规则相并作为研究对象即可,再进行近似推理。最后通过最大隶属度的最小值法得到平台暴露时间,完成系统输出的去模糊化。

假设攻击面数学期望 $\overline{E}=3.29$,$S=8.58$,则分别代入两隶属度函数可求得:数学期望属于大(E_L)和中(E_M)两模糊子集,漏洞评估分数属于大(S_L)和中(S_M)两模糊子集,且 $E_M(3.29)=0.903$,$E_L(3.29)=0.097$,$S_M(8.58)=0.284$,$S_L(8.58)=0.716$。由表 3 模糊控制的具体规则可推得,暴露时间满足第(1)、(2)、(4)、(5)条规则。取对应的 4 个模糊子集的并集作为集合。每一条规则中,通过“与”操作可得隶属度为:$\min(0.097,0.716)=0.097$,$\min(0.903,0.716)=0.716$,$\min(0.097,0.284)=0.097$,$\min(0.903,0.284)=0.284$,最大隶属度为 0.716 并处于 $S(2)$子集,将 0.716 代入到 $S(t)$中,求得 $t_1=1.432$ min,$t_2=2.852$ min,因此 t_1 即为所求的最小值。

3 仿真分析

3.1 仿真环境及参数设置

首先利用 Nessus 对在线模式下的虚拟服务器进行漏洞扫描,并记录下漏洞数量为 k_i,再利用国家信息安全漏洞库中的漏洞分级规范逐一对漏洞进行定量评估。表 4 为 Web 虚拟服务器构成。

表 4 Web 虚拟服务器构成

名称	虚拟化平台	操作系统	Web 服务器软件	Web 应用程序
Web 服务器 1	VMware	AIX	Apache	J2EE
Web 服务器 2	ESX	FreeBSD	Apache	PHP
Web 服务器 3	Virtualbox	Ubuntu Server Edition10	Tomcat	ASP
Web 服务器 4	VMware	FreeBSD	Tomcat	J2EE
Web 服务器 5	ESX	Red Hat Enterprise Linux 6	Nginx	PHP
Web 服务器 6	Virtualbox	AIX	Nginx	ASP
Web 服务器 7	VMware	Windows 7	IIS	J2EE
Web 服务器 8	ESX	Windows Server 2008	IIS	ASP
Web 服务器 9	Virtualbox	Windows Server 2016	IIS	PHP

按照表 4,构造出 9 种不同的虚拟服务器后,逐一对在线模式下的虚拟服务器的攻击面进行计量,同时对软件栈中的漏洞进行评估。再将 2 个数据输入到 Matlab 中的 Fuzzy logic designer,经过仿真即可得到平台暴露时间。

在 Matlab 中找到 Fuzzy logic designer 的应用程序,首先添加一个输入量并对两输入进行重命名,再确定其各自的 Range。分别对输入/输出量进行双击,按照上文既定的隶属度函数进行设置,编译模糊规则,最终得到仿真结果。

3.2 仿真结果分析

在仿真中,在攻击面数学期望和漏洞评估分数的区间内,任意给定一组数据,可得到服务器的最大可暴露时间。如图 3 所示,给定 77 组数据,绘制成三维散点图。根据图中点的分布情况,不难发现漏洞评估分数对虚拟服务器暴露时间的影响确实大于

攻击面数学期望的影响，攻击面数学期望越大，漏洞评估分数越高，在尽量保证虚拟服务器不被攻破的情况下，最大可暴露时间越短。

通过仿真，可以先对攻击面和漏洞评估做定量分析，再通过模糊控制器在保证系统安全的情况下计算出服务器的最大可暴露时间，最终保证系统在不消耗过多资源的情况下，防御收益尽可能大。

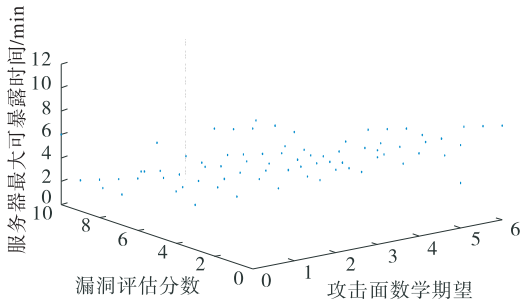

图 3　最大隶属度最小值法散点图

4　结语

本文在平台层移动目标防御的背景下，利用模糊控制相关思想和方法，以虚拟服务器遭受攻击时的攻击面数学期望和操作系统漏洞的评估分数为输入，输出平台最大暴露时间，从而为更好地进行网络防御提供了相关的参考指标。下一步的工作主要是结合网络中具体的情况，不断改进完善模型，提高准确性与可操作性。

参考文献

[1] 杨林，于全. 动态赋能网络空间防御[M]. 北京：人民邮电出版社，2016.

[2] 刘江，张红旗，杨英杰，等. 基于主机安全状态迁移模型的动态网络防御有效性评估[J]. 电子与信息学报，2017，39(3)：509-517.

[3] HUANG Y，GHOSH A K. Introducing Diversity and Uncertainty to Create Moving Attack Surfaces for Web Services[M]// JAJODIA S，GHOSH A. K，SWARUP V，et al. Moving Target Defense Creating Asymmetric Uncertainty for Cyber Threats. New York：Springer，2011：131-151.

[4] 赵鑫. 跳变信息服务系统研究[J]. 软件，2018，39(3)：204-208.

[5] 马润年，陈彤睿，王刚，等. 面向隔离区异构平台的动态防御主动迁移策略[J]. 火力与指挥控制，2019，44(3)：1-8，22.

[6] 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.

[7] OKHRAVI H，RIOADAN J，CARTER K. Quantitative Evaluation of Dynamic Platform Techniques as a Defensive Mechanism[C]//Research in Attacks，Intrusions，and Defenses. Sweden：Springer，2014：405-425.

[8] 何军. 基于云计算的 Web 防御系统研究[J]. 网络安全技术与应用，2017(3)：81-82.

[9] 王鹏，李克文. 面向 Web 服务的动态可信性评估模型[J]. 计算机系统应用，2019，28(3)：185-190.

[10] 谭韧，殷肖川，焦贤龙，等. 一种软件定义 APT 攻击移动目标防御网络架构[J]. 山东大学学报(理学版)，2018，53(1)：38-45.

[11] 刘江，张红旗，代向东，等. 基于端信息自适应跳变的主动网络防御模型[J]. 电子与信息学报，2015，37(11)：2642-2649.

[12] ZHUANG R，DELOACH S A，OU X. Towards a Theory of Moving Target Defense[C]//Proceedings of the First ACM Workshop on Moving Target Defense. Scottsdale，AZ，USA：ACM，2014：31-40.

[13] 杨林，张义荣，杨峰，等. 基于攻击面度量的动态目标防御效能评估方法[J]. 指挥与控制学报，2015，1(4)：453-457.

[14] 赵金雄，张驯，朱小琴，等. 多样化环境下的移动目标防御方法探究[J]. 电力信息与通信技术，2018，16(5)：1-5.

[15] 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.

[16] SATYA G V，SAILIK S，SUBBARAO K. Moving Target Defense for Web Applications Using Bayesian Stackelberg Games[C]// Proceedings of the 15th International Conference on Autonomous Agents and Mulltiagent. Singapor：[s. n.]，2016：1377-1378.

[17] CAI G L，WANG B S，HU W，et al. Moving Target Defense：State of the Art and Characteristics[J]. Frontiers of Information Technology & Electronic Engineering，2016，17(11)：1122-1153.

（编辑：徐楠楠）