·网络空间安全专题· 文章编号:1000-3428(2018)10-0042-04 文献标志码:A 中图分类号:TP391

动态异构冗余系统的安全性分析

王 伟[1],曾俊杰[2],李光松[1],斯雪明[1],杨本朝[1]

(1. 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;
2. 郑州大学 西亚斯国际学院文理学院,郑州 450001)

摘 要: 威胁网络空间安全的主要原因是漏洞和后门问题。为解决网络空间中基于未知漏洞、后门或病毒木马等不确定性的威胁,针对拟态防御的典型架构——动态异构冗余(DHR)系统,建立概率数学模型。从输出一致率、系统攻击成功率等角度讨论系统的安全性,通过对模型的求解和分析,得到 DHR 系统的攻击成功率的表达式,并给出 DHR 系统的性质。分析结果表明,DHR 系统的抗攻击能力优于静态异构冗余系统。

关键词: 拟态防御;动态异构冗余;漏洞;后门;主动防御

中文引用格式: 王 伟,曾俊杰,李光松,等. 动态异构冗余系统的安全性分析[J]. 计算机工程,2018,44(10):42-45,50.

英文引用格式: WANG Wei, ZENG Junjie, LI Guangsong, et al. Security analysis of dynamic heterogeneous redundant system[J]. Computer Engineering, 2018, 44(10):42-45, 50.

Security Analysis of Dynamic Heterogeneous Redundant System

WANG Wei[1], ZENG Junjie[2], LI Guangsong[1], SI Xueming[1], YANG Benchao[1]

(1. State Key Laboratory of Mathematical Engineering and Advanced Computing, Information Engineering University, Zhengzhou 450001, China; 2. Sias International University, Zhengzhou University, Zhengzhou 450001, China)

【Abstract】 The main causes of threats to cyberspace security are vulnerabilities and backdoor problems. In order to solve the threats based on unknown vulnerabilities, backdoor or virus Trojans in cyberspace, a probabilistic mathematical model is established for the typical architecture of mimic defense, Dynamic Heterogeneous Redundancy (DHR) system. The security of the system is discussed from the perspective of output consistency rate and system attack success rate. Through the solution and analysis of the model, the expression of the attack success rate of the DHR system is obtained, and some properties of the DHR system are analyzed. Analysis results show that the DHR system has better anti-attack capability than the static heterogeneous redundant system.

【Key words】 mimic defense; Dynamic Heterogeneous Redundancy (DHR); vulnerability; backdoor; active defense

DOI: 10.19678/j.issn.1000-3428.0051035

0 概述

漏洞和后门问题是网络空间安全中最严重的问题之一[1]。由于利用漏洞和后门进行的网络攻击,其攻击门槛低,网络防御成本却很高,因此严重威胁着网络空间的安全。网络空间现有的防御体制和机制,对未知漏洞和后门可能带来的未知风险更是缺乏有效的主动防御手段,因而难以应对无法彻底避免的未知漏洞以及后门实施的网络攻击[2]。

由于传统信息系统的静态性、相似性等特点,使得单纯的静态保护已经不能适应动态变化的网络安全需求,其具有单一功能的静态防御技术不能够很好地保证系统的安全[2-3]。传统的网络安全框架模型存在种种潜在问题,对于网络攻击,主要采取的是被动防御的手段,随着攻击手段的日益变化,被动防御手段已无法有效应对各种安全威胁[4]。随着时间的推移,在网络对抗环境中引入动态参数[5-6]的方法逐渐被人们重视[7-8],使得网络安全防护技术正在从静态保护向动态防御方向发展[9-10]。

在计算机系统中,采用硬件同构冗余技术可有效提升系统的可靠性,但仍存在因共性故障而导致系统灾难性后果的问题,为此有研究者提出了基于非相似余度的容错/容灾技术,力图使各个部件之间

基金项目: 国家重点研发计划项目(2016YFB0800100,2016YFB0800101);国家自然科学基金创新研究群体项目(61521003);国家自然科学基金(61602512)。

作者简介: 王 伟(1984—),男,讲师、硕士,主研方向为拟态安全、区块链;曾俊杰,讲师;李光松,副教授;斯雪明,教授;杨本朝,讲师。

收稿日期: 2018-04-02 **修回日期:** 2018-05-09 **E-mail:** ntfyllyj@aliyun.com

的故障独立以避免共性故障,但其不关注在网络安全方面的应用研究[11]。入侵容忍系统采用以异构冗余为基础的“容忍”技术来解决系统的“生存”问题,以确保系统的网络信息安全,但其是在入侵检测的基础上进行的一系列分析,即该分析是在获得先验知识的前提下进行的容侵分析[12-13]。

基于此,邬江兴院士团队提出了拟态防御思想,其目的是解决网络空间中相关应用层次上的基于未知漏洞、后门或病毒木马等不确定性的威胁,而提供具有普适性的防御理论和方法[1-4],所提出的拟态防御典型构造——动态异构冗余(Dynamic Heterogeneous Redundancy,DHR)架构,其基本思想是使用功能等价的多元化或多样化软硬构件搭建运行环境,通过策略调度、重构重组和虚拟化等多维动态的不确定性机制,使得针对系统的攻击难以实施。虽然入侵容忍系统也进行系统属性的动态配置,但从功能上讲,动态配置仍属于故障恢复操作,与改变系统静态性、确定性和相似性而引入动态性来提高系统抗攻击能力不是一个范畴的事情。

为了对 DHR 系统做进一步研究,并分析 DHR 系统的安全性和抗攻击能力,本文首先介绍 DHR 系统结构,并从 l 阶一致率和系统攻击成功率的角度,在一些前提假设下建立概率数学模型,然后讨论基于漏洞或后门攻击的 DHR 系统防御的有效性,最后分析 DHR 系统的性质。

1　DHR 系统架构

DHR 系统一般由异构构件集、输入代理、动态选择算法、执行体集和表决器组成,如图 1 所示,其中异构构件集和动态选择算法是执行体集的多样性和动态性的支撑环节[14]。异构构件集的构造可以采用软硬件模块的重组、重构、虚拟化、策略调度等广义动态化技术措施实现。执行体集由策略调度算法动态地从异构构件集中选出 n 个构件体组成,执行体集中的元素称为执行体,由执行体集的构建方法可知,某个执行体就是由策略调度算法从异构构件集中选出的某个构件体。在任意时刻,DHR 系统的输入代理模块将输入复制转发给各执行体,不同执行体的运算结果同时提交给表决器进行多数表决,表决结果即为最后的系统输出。

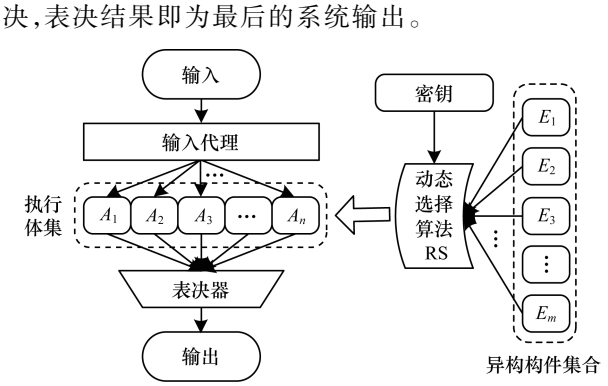

图 1　DHR 系统

在 DHR 构造机制中,允许相互独立的执行体存在一定程度的同构成分,比如操作系统可以是同一个系列的,但版本不同,这是因为 DHR 在运行环境、运行机制、调度策略、参数赋值等方面已经引入了不确定性,相互独立的执行体中即使存在某些同构成分也很难同时形成一致性或多数相同的逃逸错误。也就是说,广义动态性的导入很容易破坏非配合情况下的协同攻击,这对网络空间防御的经济性与可实现性具有重要的工程意义。因为在此情况下,可以降低对异构执行体的安全性要求,允许其“有毒带菌”运行,从而更容易构建执行体集。

DHR 架构的多数表决机制和异构构件体的策略调度机制使得执行体中存在的漏洞或后门对攻击者而言,攻击可达性大大降低。这主要有两方面的原因:DHR 机制使得攻击者需要通过变化输入激励和获取输出响应方式才能分析掌控的漏洞变得难以探测;DHR 机制使得需要通过输出矢量与攻击者交互信息的这种漏洞难以通达。DHR 机制使得动态性、多样性和随机性等不确定性技术可以基于系统架构方式集约化的实现,能够最大程度地发挥这些主动防御因素的合成效果,尤其是该机制对架构内的异构执行体没有苛刻的安全性要求,理论上各执行体允许“有毒带菌”,只要执行体集中的所有执行体不能在时空维度中表现出多数或者完全一致的错误,就不会危及 DHR 系统安全。

2　相关定义与前提假设

2.1　相关定义

记所有异构构件(简称为构件)组成的集合为 $E=\{E_1,E_2,\cdots,E_m\}$,构件 $E_i(1\leqslant i\leqslant m)$ 中所有漏洞组成集合为 V_i,所有构件中的漏洞组成的集合为 $V=\bigcup_{i=1}^{m}V_i$。动态选择算法从 m 个构件中选择 n 个构件组成当前的执行体集,如何选择构件以及何时更换执行体集由动态选择算法确定,最简单的是构件随机选择,执行体集以周期 T 更换。所有执行体集构成的集合称之为系统服务集,记为 W,W 中元素的个数称为系统服务集数 $|W|=C_m^n$。

定义 1(攻击成功)　攻击成功是指导致信息系统的机密性、可用性、完整性等遭受部分破坏的完整攻击过程。

本文模型主要探讨针对计算机系统的网络攻击,攻击成功包含若干次原子攻击,所谓原子攻击是指攻击者针对目标系统使其发生了一次输入输出操作。

在 DHR 系统中,攻击成功是指在一个执行体集周期内,攻击者造成系统“全部或多数异构执行体的输出出现完全一致的错误”,且该错误是攻击者所期望的错误。

定义 2(系统攻击成功率) 若攻击者利用 DHR 系统执行体中的漏洞发起 α 次攻击,导致系统被攻击成功 β 次,则记 $P_S=\frac{\beta}{\alpha}$为系统攻击成功率。

定义 3(l 阶输出一致率) 设某一执行体集中有 n 个执行体,若在同一输入条件下,有 l 个执行体输出相同,而且与正常输出不一致,则称该执行体集是 l 阶输出一致的。

考虑到攻击者是针对执行体中的漏洞进行的攻击,若对某漏洞 v,在 N 次攻击中有 N'次使得系统中有 l 个输出相同且与正常输出不一致,则称 $\varepsilon_l(v)=\frac{N'}{N}$是关于漏洞 v 的 l 阶输出一致率。

若忽略系统随机错误和通信误码,易知对任意漏洞 v,关于 v 的 l 阶输出一致率为:

$$\varepsilon_l(v)=\frac{\sum_{1\leqslant i_1<i_2<\cdots<i_n\leqslant m}\delta_l(i_1,i_2,\cdots,i_n,v)}{C_m^n}$$

其中,$\delta_l(i_1,i_2,\cdots,i_n,v)=\begin{cases}1,\sum_{j=1}^{n}\chi_{V_{i_j}}(v)\geqslant l\\0,\text{else}\end{cases}$,$\chi_{Set}(x)=\begin{cases}1,x\in Set\\0,x\notin Set\end{cases}$,$i_1,i_2,\cdots,i_n$ 为一个执行体集的下标编号。

漏洞 v 的 l 阶输出一致率可以看作是从漏洞的角度表示构件异构程度的一种度量。有研究者根据 NIST 国家漏洞数据库(NVD)中 11 个操作系统 2018 年来漏洞数据情况,通过研究发现某些操作系统组合的公共漏洞极少这一规律[15]。直观上同一系列的操作系统公共漏洞相对较多,而不同系列的操作系统则相对较少甚至为零。

2.2 前提假设

考虑到网络攻击过程的复杂性,对于 DHR 系统做了以下假设:

1)攻击是指基于执行体中的漏洞或后门而对系统发起的攻击,对于其他的攻击不在讨论的范围内。

2)攻击成功后必然导致输出矢量发生改变,即攻击成功后的执行体运算结果与正常执行体的运算结果相异。

3)系统的输入与输出是一一对应的,即输入和输出之间存在函数关系。

4)执行体之间是独立工作的,且表决器是安全的。

5)表决器实行多数表决,且忽略执行体集更新的时间。

3 DHR 系统建模与分析

3.1 DHR 系统建模

在 $k/n\left(k>\frac{n}{2}\right)$表决机制下,考虑攻击者针对 V 中某些漏洞 $\{v_1,v_2,\cdots,v_s\}\subseteq V$ 对 DHR 系统发起攻击,以下要计算攻击者利用漏洞 $\{v_1,v_2,\cdots,v_s\}$ 对系统攻击成功的概率。

由于不同漏洞其脆弱性是不一样的,若 v_i 的脆弱性越高,则认为漏洞 v_i 被攻击者选择的概率(频率)也就越大,因此假设在任意时刻攻击者以非零概率 $\alpha_i(\sum_{i=1}^{s}\alpha_i=1)$ 利用漏洞 v_i 发起攻击,α_i 称为漏洞 v_i 的攻击权重。对于漏洞 v_i,假设攻击者利用 v_i 对某个附有 v_i 的执行体攻击成功的概率记为 q_{v_i},系统攻击成功所需时间代价记为 t_{v_i}。

根据 DHR 架构可知,对于指定漏洞 v_i,攻击者利用 v_i 对系统进行攻击的成功概率为 $P_{v_i}=q_{v_i}\cdot\varepsilon_k(v_i)$,即攻击者对单个执行体的攻击成功概率乘以该漏洞的 k 阶一致率。

对于漏洞集合 $\{v_1,v_2,\cdots,v_s\}$,假设攻击者对系统进行了 N 次攻击,则其利用漏洞 v_i 攻击的次数估计为 $N\alpha_i$(根据不同漏洞的权重),从而在 N 次攻击中,针对漏洞 v_i,系统被攻击成功的次数估计为:

$$N_i=N\alpha_iP_{v_i}=N\alpha_i\cdot q_{v_i}\cdot\varepsilon_k(v_i)$$

因而在 N 次攻击中,系统被攻击成功的总次数估计为:

$$N'=\sum_{i=1}^{s}N_i=\sum_{i=1}^{s}N\alpha_i\cdot q_{v_i}\cdot\varepsilon_k(v_i)$$

从而系统被攻击成功的概率估计为:

$$P_S=\frac{N'}{N}=\sum_{i=1}^{s}\alpha_i\cdot q_{v_i}\cdot\varepsilon_k(v_i)=\sum_{i=1}^{s}\alpha_i\cdot q_{v_i}\cdot\frac{\sum_{1\leqslant i_1<i_2<\cdots<i_n\leqslant m}\delta_k(i_1,i_2,\cdots,i_n,v_i)}{C_m^n}$$

在 DHR 系统中,系统攻击成功率还受系统动态变化周期 T 的影响,从而对于漏洞 v,定义函数:

$$I(v)=\begin{cases}1,t_v\leqslant T\\0,t_v>T\end{cases}$$

根据定义可以看出,当系统攻击时间代价 t_v 大于系统动态变化时间 T 时,则认为系统不会被攻击成功,从而 $I(v)=0$,因此,可将系统攻击成功概率统一为:

$$P_S=\sum_{i=1}^{s}\alpha_i\cdot q_{v_i}\cdot\varepsilon_k(v_i)\cdot I(v_i)$$

3.2 结果分析

在 $k/n\left(k>\frac{n}{2}\right)$表决机制下,根据 3.1 节所求取的系统攻击成功概率表达式可以看出,DHR 系统安全性有赖于 k 阶输出一致率和系统动态变化周期 T2 个参数。

对于单个漏洞 v 来说,当攻击者利用 v 发起攻击时,若要降低系统攻击成功率,即要降低 $P_v=q_v\cdot\varepsilon_k(v)\cdot I(v)$ 值,由于 q_v 是客观存在的且与不同攻击者能力是密切相关的,因此系统很难进行改善;要降低 k 阶输出一致率 $\varepsilon_k(v)$,则需要提高系统的异构

性,即在构造执行体集时,需要使得各执行体之间的异构程度要大;欲减小 $I(v)$ 就需要减小 T,即减小系统动态变化的周期,但 T 过小,会使 DHR 系统的可用性降低,因此,需要在 DHR 系统的安全性和可用性两者平衡下选取 T 值。

对于漏洞集合 V 来说,各参数对 P_S 的影响与单个漏洞分析类似。

根据 DHR 系统攻击成功率的表达式,以下分析 P_S 的一些性质,并讨论静态异构冗余系统和 DHR 系统在抗攻击能力上的性能。

引理 1　$\delta_k(i_1,i_2,\cdots,i_n,v)\geqslant\delta_{k+1}(i_1,i_2,\cdots,i_n,v),1\leqslant k\leqslant n$。

证明:对于给定的 m、n,执行体集(对应构件下标为 $i_1,i_2,\cdots,i_n$)和任意的漏洞 v,因为

$$\delta_k(i_1,i_2,\cdots,i_n,v)=\begin{cases}1, & \sum_{j=1}^{n}\chi_{V_{ij}}(v)\geqslant k\\ 0, & \text{其他}\end{cases}$$

所以可以得出:$\sum_{j=1}^{n}\chi_{V_{ij}}(v)\geqslant k+1\Rightarrow\sum_{j=1}^{n}\chi_{V_{ij}}(v)\geqslant k$。

故 $\delta_{k+1}(i_1,i_2,\cdots,i_n,v)=1\Rightarrow\delta_k(i_1,i_2,\cdots,i_n,v)=1$,但反之不成立,因此有:

$\delta_k(i_1,i_2,\cdots,i_n,v)\geqslant\delta_{k+1}(i_1,i_2,\cdots,i_n,v)$

性质 1　P_S 是关于 k 的递减函数,其中 k 为表决阈值。

由引理 1 有:

$\delta_k(i_1,i_2,\cdots,i_n,v_i)\geqslant\delta_{k+1}(i_1,i_2,\cdots,i_n,v_i)$

从而有:

$$\sum_{1\leqslant i_1<i_2<\cdots<i_n\leqslant m}\delta_k(i_1,i_2,\cdots,i_n,v_i)\geqslant\sum_{1\leqslant i_1<i_2<\cdots<i_n\leqslant m}\delta_{k+1}(i_1,i_2,\cdots,i_n,v_i)$$

即有:

$$\frac{\sum_{i=1}^{s}\left[\alpha_i\cdot q_{v_i}\cdot I(v_i)\cdot\sum_{1\leqslant i_1<i_2<\cdots<i_n\leqslant m}\delta_k(i_1,i_2,\cdots,i_n,v_i)\right]}{C_m^n}\geqslant\frac{\sum_{i=1}^{s}\left[\alpha_i\cdot q_{v_i}\cdot I(v_i)\cdot\sum_{1\leqslant i_1<i_2<\cdots<i_n\leqslant m}\delta_{k+1}(i_1,i_2,\cdots,i_n,v_i)\right]}{C_m^n}$$

在其他参数固定的情况下,随着 k 的增加,P_S 是逐渐减小的,即 P_S 是关于 k 的递减函数。比如当 $k=n$ 时,系统表决采取 n/n 表决,即一票否决制,此时系统攻击成功率最低。但此时系统的容错能力会降低,进而增大系统的错误虚警率。

性质 2　DHR 系统优于静态异构冗余系统。

在 DHR 系统下,系统攻击成功率为:

$$P_S=\sum_{i=1}^{s}\alpha_i\cdot q_{v_i}\cdot\frac{\sum_{1\leqslant i_1<i_2<\cdots<i_n\leqslant m}\delta_k(i_1,i_2,\cdots,i_n,v_i)}{C_m^n}\cdot I(v_i)$$

在静态系统下,系统攻击成功率为:

$$P'_S=\sum_{i=1}^{s_0}\alpha_i\cdot q_{v_i}\cdot\delta_k(i'_1,i'_2,\cdots,i'_n,v_i)\cdot I(v_i)$$

其中,$(i'_1,i'_2,\cdots,i'_n)$ 为某一给定的执行体集,s_0 为执行体集 $(i'_1,i'_2,\cdots,i'_n)$ 中漏洞的总个数,因为若漏洞 v 不在执行体 $(i'_1,i'_2,\cdots,i'_n)$ 中,则有 $\delta_k(i'_1,i'_2,\cdots,i'_n,v)=0$,从而有:

$$P'_S=\sum_{i=1}^{s}\alpha_i\cdot q_{v_i}\cdot\delta_k(i'_1,i'_2,\cdots,i'_n,v_i)\cdot I'(v_i)$$

由于在静态系统下,系统动态变化周期 T 可以看成是无穷大,因此有 $I'(v_i)=1$,而在 DHR 系统下 $I(v_i)=0$ 或 1,从而有 $I(v_i)\leqslant I'(v_i)$。

由于静态系统中执行体集 $(i'_1,i'_2,\cdots,i'_n)$ 可以看成是在 DHR 系统服务集 W 中随机选择的,从而可以假设:

$$\delta_k(i'_1,i'_2,\cdots,i'_n,v_i)=\frac{\sum_{1\leqslant i_1<i_2<\cdots<i_n\leqslant m}\delta_k(i_1,i_2,\cdots,i_n,v_i)}{C_m^n}$$

从而有:

$$P_S=\sum_{i=1}^{s}\alpha_i\cdot q_{v_i}\cdot\frac{\sum_{1\leqslant i_1<i_2<\cdots<i_n\leqslant m}\delta_k(i_1,i_2,\cdots,i_n,v_i)}{C_m^n}\cdot$$

$$I(v_i)\leqslant\sum_{i=1}^{s}\alpha_i\cdot q_{v_i}\cdot\delta_k(i'_1,i'_2,\cdots,i'_n,v_i)\cdot I'(v_i)=P'_S$$

因此,从系统攻击成功率的角度可以看出,DHR 系统优于静态异构冗余系统。

4　结束语

DHR 系统是网络空间拟态防御的典型架构,本文针对 DHR 系统建立了数学模型,以 l 阶漏洞一致率、系统攻击成功率等指标表征系统的安全性,通过对模型的求解,分析了 DHR 系统的安全性和抗攻击能力。分析结果表明,DHR 系统的抗攻击能力要优于静态异构冗余系统。拟态防御机制有效性的定量分析是一个非常复杂的工作,本文对动态异构冗余系统抗网络攻击的有效性做了初步分析,但还有以下问题值得研究,如:各异构构件的异构度如何表征,假设在异构度已知的情况下选取执行体集等;在动态变化时间上,选取合适的变化间隔,使得 DHR 系统的安全性和可用性得到平衡,这将是下一步研究的问题。

参考文献

[1] 邬江兴. 网络空间拟态防御导论上册[M]. 北京:科学出版社,2017.

[2] 邬江兴. 拟态计算与拟态安全防御的原意和愿景[J]. 电信科学,2014,30(7):1-7.

[3] 邬江兴. 网络空间拟态安全防御[J]. 保密科学技术,2014(10):4-9.

[4] 邬江兴. 网络空间拟态防御研究[J]. 信息安全学报,2016,1(4):1-10.

[5] JAFARIAN J H, AI-SHAER E, DUAN Q. Openflow random host mutation:transparent moving target defense using software defined networking[C]//Proceedings of the 1st Workshop on Hot Topics in Software Defined Networks. New York,USA:ACM Press,2012:127-132.

(下转第 50 页)

[8] FEILY M,SHAHRESTNI A,RAMADASS S. A survey of Botnet and Botnet detection[C]//Proceedings of the 3rd International Conference on Emerging Security Information, Systems and Technologies. Washington D. C., USA:IEEE Press,2009:268-273.

[9] ZHAO D,TRAORE I,SAYED B,et al. Botnet detection based on traffic behavior analysis and flow intervals[J]. Computers and Security,2013,39(1):2-16.

[10] LIVADAS C, WALSH R, LAPSLEY D, et al. Usilng machine learning technologies to identify Botnet traffic[C]//Proceedings of the 31st IEEE Conference on Local Computer Networks. Washington D. C., USA: IEEE Press,2006:967-974.

[11] LIU L, CHEN S, YAN G, et al. BotTracer: execution-based bot-like malware detection[M]. Berlin, Germany: Springer,2008:97-113.

[12] STINSON E, MITCHELL C J. Characterizing bots' remote control behavior [J]. Advances in Information Security,2007,36(1):45-79.

[13] GU G,ZHANG J, LEE W. BotSniffer: detecting Botnet command and control channels in network traffic[C]// Proceedings of the 10th Network and Distributed System Security Symposium. San Diego, USA: [s. n.], 2008: 215-222.

[14] THOMAS M, MOHAISEN A. Kindred domains: detecting and clustering Botnet domains using DNS traffic [C]//Proceedings of the 23rd International Conference on World Wide Web. New York, USA: ACM Press,2014:707-712.

[15] CHOI H,LEE H. Identifying Botnets by capturing group activities in DNS traffic[J]. Computer Networks,2012, 56(1):20-33.

[16] SOLTANI S, SENO S A H, NEZHADKAMALI M, et al. A survey on real world Botnets and detection mechanisms[J]. International Journal of Information and Network Security,2014,3(2):116.

[17] STEVANOVIC M, PEDERSEN J M. An efficient flow-based Botnet detection using supervised machine learning[C]//Proceedings of 2014 International Conference on Computing, Networking and Communications. Washington D. C., USA:IEEE Press,2014:797-801.

[18] RANJAN S. Machine learning based botnet detection using real-time extracted traffic features: U. S. Patent 8, 682,812[P]. 2014-03-25.

[19] HADDADI F,PHAN D T,ZINCIR-HEYWOOD A N. How to choose from different Botnet detection systems[C]// Proceedings of IEEE/IFIP Network Operations and Management Symposium. Washington D. C., USA: IEEE Press,2016:1079-1084.

[20] YIN C,ZOU M,IKO D,et al. Botnet detection based on correlation of malicious behaviors [J]. International Journal of Hybrid Information Technology,2013,6(6): 291-300.

[21] 文传军,汪庆淼,詹永照. 隐隶属度模糊 c 均值聚类算法[J]. 计算机应用与软件,2015,32(12):245-248.

[22] SWETHA K V, SATHYADEVAN S, BILNA P. Network data analysis using spark[M]. Berlin, Germany: Springer, 2015:253-259.

[23] GARCIA S,GRILL M,STIBOREK J,et al. An empirical comparison of Botnet detection methods [J]. Computers & Security,2014,45:100-123.

编辑 索书志

(上接第 45 页)

[6] WINTEROSE M L,CARTER K M,WAGNER N,et al. Adaptive attacker strategy development aginst moving target Cyber defenses[J]. Computer Science,2014:1-11.

[7] BOSWELL T. Security evaluation and common criteria [EB/OL]. [2017-12-10]. https://link. springer. com.

[8] 樊子华,常朝稳,潘冬存. 基于 Rete 算法攻击图构建方法[J]. 计算机工程,2018,44(3):151-155,165.

[9] MADAN B B, GOSEVA-POPSTOJANOVA K. A method for modeling and quantifying the security attributes of intrusion tolerant systems[J]. Performance Evaluation,2004,56(1-4):167-186.

[10] JAJODIA S,GHOSH A K,SWARUP V,et al. Moving target defense:creating asymmetric uncertainty for cyber threats[M]. Berlin,Germany:Springer,2011.

[11] RAUSAND M. 系统可靠性理论:模型、统计方法及应用[M]. 2 版. 郭 强,王秋芳,刘树林,译. 北京:国防工业出版社,2011.

[12] 殷丽华,方滨兴. 入侵容忍系统安全属性分析[J]. 计算机学报,2006,29(8):1505-1512.

[13] 周 华,周海军,马建锋. 基于博弈论的入侵容忍系统安全性分析模型[J]. 电子与信息学报,2013,35(8): 1933-1939.

[14] 仝 青,张 铮,张为华,等. 拟态防御 Web 服务器设计与实现[J]. 软件学报,2017,28(4):883-897.

[15] GARCIA M, BESSANI A N, GASHI I. Analysis of operating system diversity for intrusion tolerance [J]. Software:Practice and Experience,2014,44(6):735-770.

编辑 索书志