一种基于概率分析的DHR模型安全性分析方法

郑秋华[1],胡程楠[1],崔婷婷[1],申延召[1],曾英佩[1],吴 铤[1,2]
(1. 杭州电子科技大学网络空间安全学院,浙江杭州 310018;2. 北京航空航天大学杭州创新研究院,浙江杭州 310051)

摘 要: 动态异构冗余(Dynamic Heterogeneous Redundancy, DHR)模型的安全性分析是拟态防御的核心问题之一.本文针对DHR模型安全性量化分析问题提出了执行体-漏洞矩阵和服务体-漏洞矩阵模型,实现了DHR系统的形式化描述.提出了攻击序列法和服务体法的两种计算方法,从系统攻击成功率和被控制率对DHR系统进行安全性分析,推导出非合谋(合谋)盲攻击和非合谋(合谋)最优攻击4种场景下安全性指标的计算公式.通过仿真实验分析了DHR模型各因素对系统安全性的影响,给出了增强DHR系统安全性的具体建议.所提方法能用于DHR系统的安全性量化分析和比较,为DHR系统构建提供量化决策支撑.

关键词: 拟态防御;动态异构冗余;安全性分析;漏洞矩阵
中图分类号: TP309.1 **文献标识码:** A **文章编号:** 0372-2112(2021)08-1586-13
电子学报URL: http://www.ejournal.org.cn **DOI:** 10.12263/DZXB.20201063

A Security Analysis Approach for Dynamic Heterogeneous Redundancy Model Based on Probability Analysis

ZHENG Qiu-hua[1], HU Cheng-nan[1], CUI Ting-ting[1], SHEN Yan-zhao[1], ZENG Ying-pei[1], WU Ting[1,2]
(1. *School of Cyberspace Security, Hangzhou Dianzi University, Hangzhou, Zhejiang* 310018, *China*;
2. *Hangzhou Innovation Institute, Beihang University, Hangzhou, Zhejiang* 310051, *China*)

Abstract: The security analysis of the dynamic heterogeneous redundancy (DHR) system is one key issue of the cyber mimic defense. We propose the executor-vulnerability matrix (MEV) and the servant-vulnerability matrix (MSV) to achieve the formal representation of the DHR system. On this basis, the attack sequence method and the servant method are proposed to analyze DHR systems' security from the attack success rate and controlled time rate. we deduce the security index calculation under (non-)collusion blind attack and (non-)collusion optimal attack scenarios. Therefore, we analyze the influence of various factors on DHR security through simulation experiments. We give several suggestions to enhance the DHR system's security. The proposed approach can be used to analyze DHR systems' security and assist in constructing DHR systems.

Key words: cyber mimic defense; dynamic heterogeneous redundancy; security analysis; vulnerability matrix

1 引言

当前网络安全处于"易攻难守"局势,目前主要防御手段本质上都是利用先验知识对已知威胁进行识别和防御,其无法有效解决漏洞、后门未知时的安全威胁,且具有一定的滞后性.对此,出现多种网络安全动态防御解决方案,以有效提高未知威胁下的系统安全水平,典型的有移动目标防御(Moving Target Defense, MTD)技术[1]和拟态防御(Cyber Mimic Defense, CMD)技术[2].CMD由邬江兴院士团队首先提出,其主要基于动态异构冗余(Dynamic Heterogeneous Redundancy, DHR)模型构建安全的信息系统.目前虽然基于DHR的拟态防御技术已在Web服务、路由调度、DNS服务[3]等多个重要领域得到了应用,但如何度量拟态DHR系统的安全性这一科学问题仍制约着拟态防御技术的落地.

对此,业界进行了积极探索.王伟等[4]基于概率模型给出了DHR系统的单次攻击成功率和多步攻击任务成功率的分析.郭威等[5]提出了可变焦有限自动机(Zooming Finite Automata, ZFA)对网络攻防过程进行

收稿日期:2020-09-25;修回日期:2021-01-25;责任编辑:王天慧
基金项目:浙江省重点研发计划(No. 2020C01078, No. 2019C01012)

建模,对传统安全技术、MTD和DHR的安全性能进行了比较分析. 朱维军等[6]提出拟态防御自动机对DHR系统进行了形式化描述,通过全状态空间搜索进行系统安全性证明. 任权等[7]利用马尔可夫链模型分析了DHR抗干扰性和系统稳态概率. 张兴明等[8]基于马尔可夫模型对攻防状态的转移关系进行建模,并通过可靠性度量验证了DHR系统的安全有效性.

但是上述方法存在需通过专家人工确定相关安全参数、只有单次攻击成功率或安全增益等安全性指标、难以用于实践指导DHR系统的构建和无法对不同DHR模型的安全性进行量化比较等不足. 针对以上问题,本文提出了一种基于概率分析的拟态DHR模型安全性量化分析方案. 主要工作有:

(1)提出执行体-漏洞矩阵和服务体-漏洞矩阵模型及构建算法,对DHR系统内在结构进行了形式化描述;

(2)基于概率分析,提出了攻击序列加权求和及各服务体安全性累加两种计算方法,解决了多次攻击度量指标的计算复杂性问题,从系统攻击成功率和被控制率维度对DHR模型进行了安全性分析,推导了不同策略下安全性指标的计算公式;

(3)提出了一种基于决策树的最优攻击序列求解算法,并通过加入虚拟安全服务体解决了求解过程中熵增益为零的计算问题;

(4)通过仿真实验分析了DHR模型各因素对系统安全性的影响,给出了增强DHR系统安全性的具体建议.

论文后续内容安排如下. 第2节介绍DHR模型安全性分析的相关工作;第3节简要介绍拟态DHR模型及DHR系统的安全性指标及定义,并在此基础上详细地分析拟态DHR系统的安全性;第4节通过仿真实验分析相关因素对系统安全性的影响,提出增强DHR系统安全性的建议,并与现有相关工作进行对比;最后对所做工作进行总结,并对后续研究工作进行展望.

2　相关工作

2.1　DHR模型安全性分析方法

DHR模型安全性分析方法主要有基于概率模型、自动机和马尔可夫模型等几类.

基于概率模型分析方法中,王伟等[4]从输出一致率、系统攻击成功率等角度讨论系统的安全性,但其工作主要局限于单次攻击成功率和基于单次攻击的多步攻击成功率分析. 李千目等[9]在给定执行体遭受攻击后出现差异和攻击者成功转移攻击等概率时,给出了求解入侵DHR各组件概率的方案,但其未给出相关概率参数的获取方法.

基于自动机的分析方法中,郭威等[8]提出ZFA进行网络攻防建模,给出一种多参数不确定的异构实现与性能分析,但目前ZFA无法刻画系统动态变化,且无法给出攻防模型中的攻击难度及防御增益完整量化. 朱维军等[6]提出拟态防御自动机,对DHR进行形式化,给出DHR形式化分析方法,把安全性自动分析规约为交替自动机模型检测问题.

基于马尔可夫模型的分析方法中,任权等[7]利用离散时间马尔可夫链分析了DHR抗干扰性能,利用连续时间马尔可夫链求解了攻击扰动条件下的稳态可用性和感知安全性. 张兴明等[8]提出了一种拟态防御马尔可夫博弈模型,分析了执行体规模、可调度空间以及防御容忍度与防御效果的关系,通过非线性规划进行了攻防博弈混合策略选择.

2.2　入侵容忍的安全性分析方法

Zhang等[10]提出了基于网络多样性的安全性评估模型和两种互补的网络多样性度量方法,并应用于网络部署. Miguel等[11]基于入侵容忍技术构建了Lazarus系统,同时提出了针对系统中共同漏洞带来风险的一系列度量标准. Katerina等[12]通过状态转移模型描述系统的动态行为,提出入侵容忍系统建模的一般方法. Luo等[13]基于马尔可夫模型和有限自动机,提出了最优状态转移模型,以提高系统的容忍度. Miguel等[14]调研了NIST 15年中记录的11种操作系统,证实了异构性的提升能显著增加系统对攻击的容忍能力.

2.3　MTD模型安全性分析方法

Massimiliano等[15]指出建立度量MTD有效性评估指标的必要性,同时提出了一种MTD的资源可用性和性能的定量评估模型,提出了性能和稳定性约束下构建攻击者成功概率最小系统的方法. Hong等[16]提出了攻击表示的分层模型,同时使用重要性度量,解决MTD部署中可伸缩性度量问题,提出了攻击效果和防御效果等MTD技术有效性的度量指标[17]. Ma等[18]提出基于漏洞熵、攻击熵、衰减熵的MTD评估模型和安全性计算方法. Hooman等[19]根据系统风险、攻击成本、攻击回报和可用性等因素建立了MTD系统评估模型,提出了多种MTD技术组合使用的部署建议.

3　基于概率分析的DHR模型安全性分析

本节首先简要介绍DHR模型,然后给出DHR模型的安全性指标及定义,再进行DHR模型的安全性分析.

3.1　DHR模型简介

DHR模型[2]是一个典型的IPO(In Process Out)模型,如图1所示,其主要由构建模块、调度模块、输入模块、处理模块和输出模块五个部分构成.

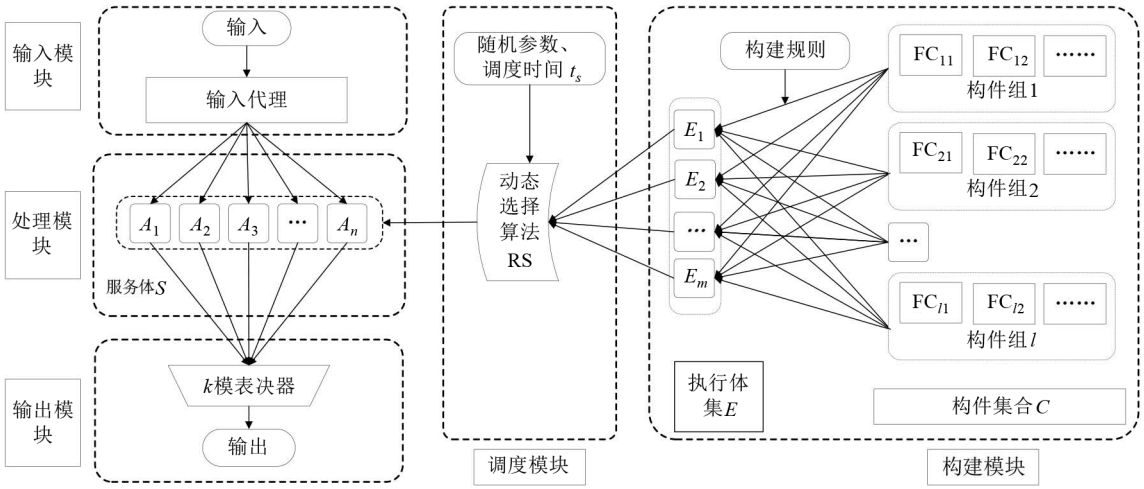


图1 DHR模型

(1) 构建模块

从l个异构功能组件FC(Function Component)集中选择组件构建系统的异构执行体集$E=\{E_i, 1\leqslant i\leqslant m\}$,其中$m$是系统异构执行体的数目. E中各异构执行体都可独立处理系统的输入请求,并返回结果.

(2) 调度模块

根据调度策略从系统异构组件集合中选择n个异构执行体,组成处理模块中的当前服务体S,参数n称为系统的服务体模. 调度策略主要包括异构执行体的选择和调度时间t_s的确定. 常用的调度策略是在异构执行体集E中随机选取n个异构执行体$A_1, A_2, \cdots, A_n$,组成服务体S. 在调度时间t_s后,服务体S的所有执行体均下线清洗还原.

(3) 输入模块

解析接收到的输入请求,生成n个输入请求并发送到处理模块.

(4) 处理模块

将n个输入请求发送到当前服务体S的n个执行体,并返回结果到输出模块.

(5) 输出模块

调用表决器对处理结果进行$k/n(n/2\leqslant k\leqslant n)$表决,若$n$个输出结果中存在$k$个及以上的一致结果,则输出该结果;否则阻断输出. 参数k称为系统判决模.

定义1 系统攻击成功率 若系统在一运行周期内被攻击成功1次,称系统该周期内被成功攻击. 设系统运行的周期数为α,其中被成功攻击的周期数为β,称$p=\alpha/\beta$为系统攻击成功率.

定义2 系统被控制率 给定系统服务序列$W=W_1\cdots W_i\cdots$和服务时序$t(w_1)\cdots t(w_i)\cdots$,若在运行周期$t(w_i)$内攻击者从$W_i$开始工作至攻击者第一次攻击成功所耗费的时间为$t_a(i)$,称$t_c(i)=t(w_i)-t_a(i)$为服务序列$W_i$中的被控制时间. 所有服务序列的被控制时间之和与运行时间之和之比$\theta=\sum_i t_c(i)/\sum_i t(w_i)$称为系统被控制率.

3.2 DHR模型的安全性分析

本节首先提出执行体-漏洞矩阵(Matrix of Executor-Vulnerability, MEV)和服务体-漏洞矩阵模型(Matrix of Servant-Vulnerability, MSV),对DHR系统的结构进行形式化描述. 上述模型基于以下出发点:攻击者对系统的观察由系统对攻击的响应所决定,若多个执行体(或服务体)针对某个特定漏洞攻击的响应一致,那么即使其内部实现细节不同,其受到该攻击后的表现是一致的.

3.2.1 执行体-漏洞矩阵MEV和服务体-漏洞矩阵MSV

首先给出执行体-漏洞矩阵模型MEV和服务体-漏洞矩阵模型MSV定义.

定义3 执行体-漏洞矩阵 对于m个执行体$E_1\cdots E_m$以及包含ω个漏洞的漏洞集合V,称$\boldsymbol{M}_{E\text{-}V}=(mev_{i,j})_{m\times\omega}$为对应的执行体-漏洞矩阵,其中

$$mev_{i,j}=\begin{cases}1, & \text{执行体}E_i\text{存在第}j\text{个漏洞}\\ 0, & \text{执行体}E_i\text{不存在第}j\text{个漏洞}\end{cases}$$

定义4 服务体-漏洞矩阵 对于r个服务体$S_1\cdots S_r$及包含ω个漏洞的集合V,称$\boldsymbol{M}_{S\text{-}V}=(msv_{i,j})_{r\times\omega}$为服务体-漏洞矩阵,其中

$$msv_{i,j}=\begin{cases}1, & \text{服务体}S_i\text{存在第}j\text{个漏洞}\\ 0, & \text{服务体}S_i\text{不存在第}j\text{个漏洞}\end{cases}$$

记m、n、k和ω分别为DHR系统的异构执行体个数、服务体模、判决模和漏洞维数,其所有的服务体个数r为组合数C_m^n. 若已知执行体-漏洞矩阵$\boldsymbol{M}_{E\text{-}V}$,则可

按如下方式得到服务体-漏洞矩阵$\boldsymbol{M}_{S-V}$.

(1)在执行体-漏洞矩阵$\boldsymbol{M}_{E-V}$中按字典序依次取出n行,形成$r = C_m^n$个子矩阵$\{\boldsymbol{M}_1, \boldsymbol{M}_2, \cdots, \boldsymbol{M}_r\}$.

(2)将每个子矩阵$\boldsymbol{M}_i$的所有行相加,得到r个行向量$\overline{\boldsymbol{M}_i}$, $1 \leqslant i \leqslant r$.

(3)对行向量$\overline{\boldsymbol{M}_i} = (m_{i1}, \cdots, m_{i\omega})$令

$$m'_{ij} = \begin{cases} 1, & m_{ij} \geqslant k \\ 0, & m_{ij} < k \end{cases}$$

则服务体-漏洞矩阵$\boldsymbol{M}_{S-V} = \left(m'_{ij}\right)_{r \times \omega}$.

3.2.2　攻击模型描述

本文的DHR安全性分析基于攻击者不了解内在结构的黑盒模型,及攻击者已知DHR系统漏洞、后门和调度策略的白盒模型. 白盒时,以下DHR系统因素是已知的.

(Ⅰ)执行体-漏洞矩阵$\boldsymbol{M}_{E-V}$和服务体-漏洞矩阵$\boldsymbol{M}_{S-V}$.

(Ⅱ)服务体的调度周期t_s和随机调度策略.

黑盒模型下,攻击者不了解系统的内部结构,本文假设此时攻击者采用盲攻击策略(等概率选择攻击序列*进行攻击). 白盒模型下,攻击者已知执行体-漏洞矩阵等细节,故本文假设此时攻击者采用最优攻击策略(选择成功率最大的攻击序列进行攻击).

此外,本文在攻击者能力最大化,即worst-case情况下分析DHR系统的安全性. 为此作如下前提假设.

(Ⅰ)系统的输入与输出一一对应.

(Ⅱ)对漏洞的成功攻击必定导致执行体输出与正常情况下的输出不一致.

(Ⅲ)不考虑通信误码、执行体故障等引起的随机错误,对某一漏洞攻击时,n个执行体输出相同(但与正常输出不一致)当且仅当n个执行体中均存在该漏洞.

(Ⅳ)攻击者对已知漏洞的攻击必定成功.

(Ⅴ)不考虑攻击响应时间及协同攻击通信时间,即设这两个时间均为0.

此外,与攻击相关的因素还包括攻击者数量、攻击者是否合谋**和攻击花费的时间.

特别要指出的是,本文DHR系统安全性分析并不在DHR自身防御能力外添加其他防御措施,而只评估由动态性、随机性和异构冗余性带来的内生安全能力.

3.2.3　DHR系统安全性分析

本节从单(多)攻击者场景对DHR系统的系统攻击成功率、被控制率安全性指标进行量化分析. 同时区分τ次攻击成功率(即τ次攻击中至少成功1次的概率)以及τ阶攻击成功率(即第τ次攻击时才成功,而之前攻击均失败的概率). 为简化分析,假设所有攻击单个漏洞的耗费时间均为t_a.

3.2.3.1　系统攻击成功概率

(1)单攻击者的τ次攻击成功概率

对服务体可能存在的至多ω个漏洞,假定攻击者每次对1个漏洞进行攻击,则攻击者实际攻击次数$\tau \leqslant \omega$. 由于在这τ次攻击中,其所针对的τ个漏洞共有P_ω^τ种排列方式,其中P_ω^τ表示排列数(若$\omega < \tau$,则令$P_\omega^\tau = 0$),故τ次攻击只有P_ω^τ个可能的攻击序列. 记这些攻击序列所组成的集合为$\Gamma(\tau) = \{A_\tau^i, i = 1, \cdots, P_\omega^\tau\}$. 对于攻击序列$A_\tau^i$,若其攻击的漏洞序列为$v_{i_1}, \cdots, v_{i_\tau}$,则其攻击成功概率为当前服务体中存在$v_{i_1}, \cdots, v_{i_\tau}$中任一漏洞的概率. 对于服务体-漏洞矩阵$\boldsymbol{M}_{S-V}$而言,记第$i_1, \cdots, i_\tau$列分量至少有一个等于1的行向量的个数为$|\mathrm{R}(\boldsymbol{M}_{S-V}, A_\tau^i)|$,则攻击序列$A_\tau^i$的成功概率$\mathrm{SPr}(A_\tau^i)$为

$$\mathrm{SPr}(A_\tau^i) = \frac{|\mathrm{R}(\boldsymbol{M}_{S-V}, A_\tau^i)|}{C_m^n} \tag{1}$$

记$\Pr(A_\tau^i)$为选择攻击序列A_τ^i的概率,则τ次攻击的攻击成功率为

$$\mathrm{SPr}(\Gamma(\tau)) = \sum_{A_\tau^i \in \Gamma(\tau)} \Pr(A_\tau^i) \times \mathrm{SPr}(A_\tau^i) \tag{2}$$

从式(2)中可得,对于ω个系统漏洞,τ次攻击成功率的计算复杂度为$O(P_\omega^\tau)$. DHR系统包含的漏洞数目通常较多,以拟态Web系统为例,其涉及漏洞约4500个[20],对应10次攻击序列数约为3.37×10^{36},故通过式(2)求解τ次攻击成功率计算上并不可行.

对此,本文提出了一种先分别计算各服务体的τ次攻击成功率,然后将其进行加权平均的方法来计算$\mathrm{SPr}(\Gamma(\tau))$. 记$S_i$中的漏洞数为$\eta_i$,则对服务体$S_i$进行$\tau$次攻击全部失败的攻击序列数为$P_{\omega-\eta_i}^{\tau}$***,故对服务体$S_i$进行$\tau$次攻击均失败的概率$\mathrm{FPr}_\tau(S_i)$为

$$\mathrm{FPr}_\tau(S_i) = \frac{P_{\omega-\eta_i}^{\tau}}{P_\omega^\tau} \tag{3}$$

其中η_i为服务体S_i中存在的漏洞数目,P_ω^τ为所有τ次攻击序列的个数.

基于式(3),可得盲攻击时攻击者对服务体S_i的τ次攻击成功概率为

---

* 攻击序列指攻击者的一系列攻击手段所组成的序列.

** 非合谋攻击是指各攻击者同时单独进行攻击,不共享攻击策略和攻击响应. 合谋攻击是指各攻击者同时对系统进行攻击,且共享攻击策略和攻击响应. 当某一攻击失败后,所有合谋攻击者均会根据此时的系统响应进行调整.

*** 要注意的是,在考虑的攻击序列中,所针对的漏洞是有序排列的,因此所对应的为排列数而非组合数.

$$\mathrm{SPr}_{\tau}(S_i)=1-\frac{P_{\omega-\eta_i}^{\tau}}{P_{\omega}^{\tau}} \tag{4}$$

盲攻击时，各服务体被选概率均为$1/C_m^n$，故由式(4)可得τ次攻击成功率SPr_{τ}.

$$\mathrm{SPr}_{\tau}=\sum_{i=1}^{C_m^n}\frac{\mathrm{SPr}_{\tau}(S_i)}{C_m^n}=\frac{\sum_{i=1}^{C_m^n}\left(1-\dfrac{P_{\omega-\eta_i}^{\tau}}{P_{\omega}^{\tau}}\right)}{C_m^n} \tag{5}$$

基于式(5)的SPr_{τ}计算复杂度为$O(C_m^n)$. 因为系统成本等因素，DHR系统的执行体个数m和服务体选择模n通常都较小，因此式(5)比式(2)具有更高的计算效率.

(2)单攻击者的τ次最优攻击成功概率

为了度量白盒时的系统安全性，考虑最大攻击成功率，即已知服务体-漏洞矩阵$\boldsymbol{M}_{S-V}$时，选择成功率最大的τ漏洞序列进行攻击. 记A_{τ}^{*}为成功率最大的攻击序列，则由式(1)可知τ次攻击序列最大成功率为

$$\mathrm{SPr}_{\tau}^{*}=\max(\mathrm{SPr}(\mathrm{A}_{\tau}))=\frac{|\mathrm{R}(\boldsymbol{M}_{S-V},A_{\tau}^{*})|}{C_m^n} \tag{6}$$

为找出成功概率最大的攻击序列，本文基于决策树算法ID3[21]提出了一种基于信息增益的最优攻击序列选取算法(Optimal Attack Sequence Solve Algorithm base-on Information Gain, OAS-IG)(见算法1). 对信息增益进行度量的指标，如矩阵$\boldsymbol{M}_{S-V}$的熵、漏洞v_i的熵增益等，其定义如式(7).

$$\begin{aligned}\mathrm{Ent}(\boldsymbol{M}_{S-V})&=-(\mathrm{I}(\boldsymbol{M}_{S-V})\times\ln(\mathrm{I}(\boldsymbol{M}_{S-V}))\\&\quad+(1-\mathrm{I}(\boldsymbol{M}_{S-V}))\\&\quad\times\ln(1-\mathrm{I}(\boldsymbol{M}_{S-V})))\\\mathrm{I}(\boldsymbol{M}_{S-V})&=\frac{C-V(\boldsymbol{M}_{S-V})}{C-S(\boldsymbol{M}_{S-V})}\\\mathrm{Gain}(\boldsymbol{M}_{S-V},v_i)&=\mathrm{Ent}(\boldsymbol{M}_{S-V})\\&\quad-\frac{C-V(\boldsymbol{M}_{S-V},v_i)}{C-S(\boldsymbol{M}_{S-V})}\times\mathrm{Ent}(\boldsymbol{M}_{S-V},v_i)\end{aligned} \tag{7}$$

其中$C-S(\boldsymbol{M}_{S-V})$、$C-V(\boldsymbol{M}_{S-V})$分别为$\boldsymbol{M}_{S-V}$中所有服务体的个数和存在漏洞的服务体个数，$S-R(\boldsymbol{M}_{S-V},v_i)$表示由$\boldsymbol{M}_{S-V}$中所有不存在漏洞$v_i$的服务体组成的服务体-漏洞矩阵，$\mathrm{Ent}(\boldsymbol{M}_{S-V},v_i)=\mathrm{Ent}(S-R(\boldsymbol{M}_{S-V},v_i))$为漏洞$v_i$的漏洞熵.

若所有服务体都存在安全漏洞，即$\boldsymbol{M}_{S-V}$中不存在全为0的行向量，将会导致所有漏洞的熵增益都为零. 为此在服务体-漏洞矩阵中引入了一个虚拟的安全服务体，即在$\boldsymbol{M}_{S-V}$矩阵中增加一个全0的行向量.

(3)多攻击者时的系统攻击成功率

记t_s为系统调度时间，ω为漏洞数. 以下分析多攻击者不同策略时攻击成功率.

算法1 τ次最优攻击序列选取算法(OAS-IG)

输入：服务体-漏洞矩阵**MSV**，τ
输出：最优攻击序列OAS
$i\leftarrow 0$, OAS $\leftarrow\varnothing$
while i小于τ或**MSV**不为空且非全零do
  mostIVs $\leftarrow\varnothing$
  将所有攻击成功率最大的漏洞v加入mostIVs
  if mostIVs 中只包含一个漏洞 **then**
    将该漏洞添加到OAS中
  else
    if 最大的漏洞熵增益maxVEG为0 **then**
      返回最优攻击序列OAS
    endif
    选择熵增益最大的漏洞$v_{\max}$VEG加入OAS
    在**MSV**中去除包含漏洞$v_{\max}$VEG的服务体
  endif
  $i\leftarrow i+1$
end while
返回最优攻击序列OAS

(a)非合谋盲攻击.

非合谋时，攻击者对服务体的最大有效攻击次数$\tau_{\max-s}$为$\min(\omega,\lceil t_s/t_a\rceil)$. 因各攻击者失败概率为$\mathrm{FPr}_{\tau}^{i}$，故此时攻击成功率为

$$\begin{aligned}\mathrm{SPr}_{\tau_{\max-s}}^{N}&=1-\mathrm{FPr}_{\tau_{\max-s}}^{N}\\&=1-\left(1-\frac{\sum_{i=1}^{C_m^n}\left(1-\dfrac{P_{\omega-\eta_i}^{\min(\omega-\eta_i,\tau_{\max-s})}}{P_{\omega}^{\tau_{\max-s}}}\right)}{C_m^n}\right)^{N}\end{aligned} \tag{8}$$

其中$\mathrm{FPr}_{\tau_{\max-s}}^{N}$是指$N$个攻击者对系统进行$\tau_{\max-s}$次攻击都失败的概率.

(b)非合谋最优攻击.

非合谋时攻击者将选择相同的τ个漏洞进行攻击，此时攻击成功率与单攻击者的最优攻击成功率相同，如式(6)所示.

(c)合谋盲攻击.

因最大有效攻击次数$\tau_{\max-c}$为$\min(\omega,N\times\lceil t_s/t_a\rceil)$，故可得攻击成功率.

$$\mathrm{SPr}_{\tau_{\max-c}}^{N}=\frac{1}{C_m^n}\times\sum_{i=1}^{C_m^n}\left(1-\frac{P_{\omega-\eta_i}^{\min(\omega-\eta_i,\tau_{\max-c})}}{P_{\omega}^{\tau_{\max-c}}}\right) \tag{9}$$

其中η_i是指服务体-漏洞矩阵$\boldsymbol{M}_{S-V}$中服务体S_i中存在的漏洞数目.

(d)合谋最优攻击.

此时最大有效攻击次数也为$\tau_{\max-c}$，因此由式(6)可得攻击成功率为

$$\mathrm{SPr}_{\tau_{\max-c}}^{N}=\frac{|\mathrm{R}(\boldsymbol{M}_{S-V},A_{\tau_{\max-c}}^{*})|}{C_m^n} \tag{10}$$

其中$|\mathrm{R}(\boldsymbol{M}_{S-V}, A^*_{\tau_{\max-c}})|$表示矩阵$\boldsymbol{M}_{S-V}$中包含$A^*_{\tau_{\max-c}}$中任一漏洞的服务体的个数.

3.2.3.2　系统被控制率

系统控制率的计算公式为

$$\theta = \sum_{i=1}^{\infty} \frac{t_s - i \times t_a}{t_s} \times \mathrm{O-SPr}_\tau \tag{11}$$

其中$\mathrm{O-SPr}_\tau$为τ阶攻击成功率,即攻击者仅第τ轮攻击成功,而之前攻击均失败的概率.

以下分析不同攻击策略时的τ阶攻击成功率$\mathrm{O-SPr}_\tau$.

(1)τ阶攻击成功率

(a)盲攻击时单攻击者的τ阶攻击成功率.

对于针对τ个不同漏洞的攻击序列集$\Gamma(\tau) = \{A^i_\tau, i = 1, \cdots, P^\tau_\omega\}$,记$\Pr(A^i_\tau)$为选择攻击序列$A^i_\tau$的概率,$\mathrm{O-SPr}_\tau(A^i_\tau)$为攻击序列$A^i_\tau$的$\tau$阶攻击成功率,则采用攻击序列集$\Gamma(\tau)$的$\tau$阶攻击成功率为

$$\mathrm{O-SPr}_\tau(\Gamma(\tau)) = \sum_{A^i_\tau \in \Gamma(\tau)} \Pr(A^i_\tau) \times \mathrm{O-SPr}_\tau(A^i_\tau) \tag{12}$$

其计算复杂度与式(2)相同均为$O(P^\tau_\omega)$. 与3.2.3.1节类似,以下采用先计算各个服务体的τ阶攻击成功率,然后进行加权平均的方式以减少计算量.

服务体S_i的τ阶攻击成功率$\mathrm{O-SPr}_\tau(S_i)$相当于从与S_i无关及相关漏洞中各选取$\tau-1$、1个漏洞所组成的序列之比,即

$$\mathrm{O-SPr}_\tau(S_i) = \frac{\eta_i \times P^{\tau-1}_{\omega-\eta_i}}{P^\tau_\omega} \tag{13}$$

其中η_i为服务体S_i中存在的漏洞数目.

若等概率选择各服务体,由式(13)得

$$\mathrm{O-SPr}_\tau = \frac{1}{C^n_m} \sum_{i=1}^{C^n_m} \frac{\eta_i \times P^{\tau-1}_{\omega-\eta_i}}{P^\tau_\omega} \tag{14}$$

(b)单攻击者最优攻击时的τ阶攻击成功率.

当攻击者已知服务体-漏洞矩阵$\boldsymbol{M}_{S-V}$,选择τ阶攻击成功率最大的漏洞序列$v_{i_1}, \cdots, v_{i_\tau}$所对应的攻击序列$A^*_\tau$进行攻击时,$\tau$阶攻击序列最大成功概率为

$$\mathrm{O-SPr}_\tau = \max(\mathrm{O-SPr}_\tau(A^i_\tau)) = \frac{|\mathrm{O-R}(\boldsymbol{M}_{S-V}, A^*_\tau)|}{C^n_m} \tag{15}$$

其中$|\mathrm{O-R}(\boldsymbol{M}_{S-V}, A^*_\tau)|$表示服务体-漏洞矩阵$\boldsymbol{M}_{S-V}$中仅包含漏洞$v_{i_\tau}$且不包含$v_{i_1}, \cdots, v_{i_{\tau-1}}$的服务体数目.$\tau$阶最优攻击序列的选取算法类似于算法1.

(c)多攻击者非合谋盲攻击时的τ阶攻击成功率.

当攻击者等概率选取漏洞并独立攻击时,记服务体S_i的漏洞数为η_i,则任一攻击者前$\tau-1$次攻击均失败有$P^{\tau-1}_{\omega-\eta_i}$种,而第$\tau$次攻击成功或失败分别有$\eta_i$和$\omega-\eta_i-(\tau-1)$种,故$N$个攻击者前$\tau-1$次攻击失败后再进行第$\tau$次攻击的可能数为$(P^{\tau-1}_{\omega-\eta_i} \times \eta_i + P^\tau_{\omega-\eta_i})^N$. 所有攻击者$\tau$次攻击均失败的可能有$(P^\tau_{\omega-\eta_i})^N$种,恰在第$\tau$次攻击才成功的可能数为两者之差. 综上,可得服务体S_i在N攻击者非合谋盲攻击时的τ阶攻击成功率为

$$\mathrm{O-SPr}^N_\tau(S_i) = \frac{(P^{\tau-1}_{\omega-\eta_i} \times \eta_i + P^\tau_{\omega-\eta_i})^N - (P^\tau_{\omega-\eta_i})^N}{(P^\tau_\omega)^N} \tag{16}$$

若等概率选择各服务体,由式(16)可得

$$\mathrm{O-SPr}^N_\tau = \frac{1}{C^n_m} \sum_{i=1}^{C^n_m} \frac{(P^{\tau-1}_{\omega-\eta_i} \times \eta_i + P^\tau_{\omega-\eta_i})^N - (P^\tau_{\omega-\eta_i})^N}{(P^\tau_\omega)^N} \tag{17}$$

(d)多攻击者非合谋最优攻击时的τ阶攻击成功率.

此时各攻击者都选择最优攻击序列进行攻击,故N攻击者非合谋最优攻击的τ阶攻击成功率同单攻击者的最优攻击τ次阶攻击成功率,如式(15)所示.

(e)多攻击者合谋盲攻击时的τ阶攻击成功率.

此时攻击者彼此分享攻击策略以及攻击结果,可假定针对指定漏洞的攻击至多进行一次,故$\tau-1$轮合谋攻击所针对的漏洞数至多为$(\tau-1)\times N$,可得对服务体S_i的前$\tau-1$轮攻击失败的可能有$P^{(\tau-1)\times N}_{\omega-\eta_i}$种,而第$\tau$轮攻击成功的次数有1至$N$种. 第$\tau$轮进行攻击次数为$N$且成功攻击次数为$j$的可能有$C^j_N$种,对应的攻击序列有$P^j_{\eta_i} \times P^{N-j}_{\omega-\eta_i-(\tau-1)\times N}$种,故第$\tau$轮成功$j$次的攻击序列共有$C^j_N \times P^j_{\eta_i} \times P^{N-j}_{\omega-\eta_i-(\tau-1)\times N}$种. 因盲攻击时各漏洞被等概率选取,故服务体$S_i$在$N$攻击者非合谋盲攻击时的$\tau$阶成功率为

$$\mathrm{O-SPr}^N_\tau(S_i) = \frac{\sum_{j=1}^{N}(C^j_N \times P^j_{\eta_i} \times P^{\tau\times N-j}_{\omega-\eta_i})}{P^{\tau\times N}_\omega} \tag{18}$$

当等概率选择服务体时,由式(18)可得

$$\begin{aligned}\mathrm{O-SPr}^N_\tau &= \frac{1}{C^n_m} \sum_{i=1}^{C^n_m} \mathrm{O-SPr}^N_\tau(S_i) \\ &= \frac{1}{C^n_m} \sum_{i=1}^{C^n_m} \frac{\sum_{j=1}^{N}(C^j_N \times P^j_{\eta_i} \times P^{\tau\times N-j}_{\omega-\eta_i})}{P^{\tau\times N}_\omega}\end{aligned} \tag{19}$$

(f)多攻击者合谋最优攻击时的τ阶攻击成功率.

合谋最优攻击时,设第τ轮的第i次攻击才成功,则该事件发生概率为$\mathrm{O-SPr}^*_{(\tau-1)\times N+i}$. 故可得合谋最优攻击时$\tau$阶攻击成功概率为

$$\begin{aligned}\mathrm{O-SPr}^N_\tau &= \sum_{k=(\tau-1)\times N+1}^{\tau\times N} \mathrm{O-SPr}^*_k \\ &= \sum_{k=(\tau-1)\times N+1}^{\tau\times N} \frac{|\mathrm{O-R}(\boldsymbol{M}_{S-V}, A^*_k)|}{C^n_m}\end{aligned} \tag{20}$$

式中$|\mathrm{O-R}(\boldsymbol{M}_{S-V}, A^*_k)|$表示矩阵$\boldsymbol{M}_{S-V}$中仅包含攻击序列$A^*_k$中第$k$个漏洞的服务体数目.

(2)系统控制率计算

(a)单攻击者盲攻击时的系统控制率.

因针对系统的最大攻击次数 $\tau_{\max\text{-}s}=\min(\omega,\lceil t_s/t_a\rceil)$,由式(11)、式(14)可得此时的系统控制率.

$$\theta=\sum_{i=1}^{\tau_{\max\text{-}s}}\left(\frac{t_s-i\times t_a}{t_s}\times\frac{1}{C_m^n}\sum_{j=1}^{C_m^n}\frac{\eta_j\times P_{\omega-\eta_j}^{i-1}}{P_\omega^i}\right)\tag{21}$$

(b)单攻击最优攻击场景下的系统控制率.

因攻击系统的最大次数也为 $\tau_{\max\text{-}s}$,由式(11)、式(15)可得此时的系统控制率.

$$\theta=\sum_{i=1}^{\tau_{\max\text{-}s}}\frac{t_s-i\times t_a}{t_a}\times\frac{|\mathrm{O}-\mathrm{R}(\boldsymbol{M}_{S\text{-}V},A_i^*)|}{C_m^n}\tag{22}$$

(c)多攻击者非合谋盲攻击时的系统控制率.

此时最大攻击轮数也为 $\tau_{\max\text{-}s}$,由式(11)、式(17)可得此时的系统控制率.

$$\theta=\sum_{i=1}^{\tau_{\max\text{-}s}}\left(\frac{t_s-i\times t_a}{t_s}\times\mathrm{O}-\mathrm{SPr}_i^N\right)\tag{23}$$

(d)多攻击者非合谋最优攻击时的系统控制率.

非合谋时攻击者彼此独立地发动攻击,其系统控制率同单攻击者最优攻击,此时的系统控制率如式(22)所示.

(e)多攻击者合谋盲攻击时的系统控制率.

此时由于攻击者不会对同一漏洞进行多次攻击,因此对系统的最大攻击轮数 $\tau_{\max\text{-}c}=\min(\lceil\omega/N\rceil,\lceil t_s/t_a\rceil)$. 由式(11)、式(19)可得此时的系统控制率如式(24).

$$\theta=\sum_{i=1}^{\tau_{\max\text{-}c}}\left(\frac{t_s-i\times t_a}{t_s}\times\frac{1}{C_m^n}\sum_{j=1}^{C_m^n}\frac{\sum_{k=1}^{\min(N,\omega-(i-1)\times N)}(C_N^k\times P_{\eta_j}^k\times P_{\omega-\eta_j}^{\min(i\times N,\omega)-k})}{P_\omega^{\min(\omega,i\times N)}}\right)\tag{24}$$

(f)多攻击者合谋最优攻击时的系统控制率.

此时攻击者对系统的最大攻击轮数也为 $\tau_{\max\text{-}c}$. 由式(11)、式(20)可得此时的系统控制率如式(25).

$$\theta=\sum_{i=1}^{\tau_{\max\text{-}c}}\left(\frac{t_s-i\times t_a}{t_s}\times\sum_{k=1}^{\min(N,\omega-(i-1)\times N)}\frac{|\mathrm{O}-\mathrm{R}(\boldsymbol{M}_{S\text{-}V},A_{(i-1)\times N+k}^*)|}{C_m^n}\right)\tag{25}$$

3.2.4 特定DHR模型的安全性比较

(1) 单执行体系统

单执行体系统等效于 $m=1,n=1,k=1,t_s=\infty$ 的DHR系统. 其执行体-漏洞矩阵与服务体-漏洞矩阵相同,记单执行体系统中的漏洞数为 $\eta(1\leqslant\eta\leqslant\omega)$. 黑盒时,攻击 $\omega-\eta+1$ 次中至少有1次成功攻击,其系统攻击成功率为 $p\geqslant(\infty-\omega-\eta+1)\approx1$,同理可得系统控制率 $\theta\geqslant(\infty-\omega-\eta+1)/\infty\times(\infty-\omega-\eta+1)/\infty\approx1$. 白盒时,攻击者任意选择 η 个漏洞之一,就可成功攻击. 这说明若单执行体系统存在漏洞,则理论上系统必然会被攻陷控制. 因此单执行体自身防御的有效措施只能是漏洞修补.

(2) 3模静态同构系统

3模静态同构系统等同 $m=3,n=3,k=2,t_s=\infty$ 的DHR系统,其执行体漏洞矩阵与单执行体的服务体漏洞矩阵相同,其安全性同单执行体系统.

(3) 3模静态异构冗余系统

3模静态异构冗余系统等效于 $m=3,n=3,k=2,t_s=\infty$ 的DHR系统,其服务体数目为1. 3模静态异构冗余系统的服务体-漏洞矩阵主要取决于各执行体之间的漏洞异构性. 当各执行体之间不存在相同的漏洞时,其服务体不存在任何漏洞,系统攻击成功率为0,控制率也为0. 除此之外,3模静态异构冗余系统的安全性等同于由其单一服务体组成的单执行体系统.

(4) 单模动态异构冗余系统

单模动态异构冗余系统等效于 $n=1,k=1$ 的DHR系统. 单模动态异构冗余系统的服务体-漏洞矩阵与执行体-漏洞矩阵相同,因为其服务体-漏洞矩阵中的漏洞更多,故其安全性比多模动态异构冗余系统低.

如上所述,DHR系统比传统的防御技术均具有更好的安全性.

4 实验和分析

本节通过仿真实验从系统攻击成功率和被控制率维度分析 $\{p,\omega,m,n,k,N,t_s/t_a\}$ 等因素在不同攻击策略下对DHR系统安全性的影响. 实验方案主要包括执行体-漏洞矩阵生成、服务体-漏洞矩阵生成和攻击成功率及被控制率计算三个步骤,具体设计方案在后续部分给出. 各参数的取值范围根据系统安全性与构建成本和运行效率综合均衡的原则进行选取.

4.1 漏洞概率 p 对系统安全性的影响

实验设计如方案1.

实验参数设置为 $\omega=1000,m=30,n=3,k=2,N=20,t_s/t_a=20,H=100000$. 漏洞出现概率 p 的取值范围为 $\{0.01,0.06,\cdots,0.15\}$,对应漏洞个数均值为10至150,该取值范围覆盖了漏洞率从低到高的多种场景. 图2为实验结果.

如图2所示,漏洞发生率与系统安全性呈负相关,这是因为执行体漏洞增加会导致服务体漏洞增加,进而降低系统安全性. 图2(a)中,当 p 大于0. 09时,各攻击策略下的系统攻击成功率均接近1. 这说明须限制系统漏洞数,否则即使黑盒,仍可通过暴力攻破系统.

方案1

1 给定参数$\{\omega, m, n, k, N, t_s/t_a\}$和$\{p\}$.

2 重复步骤(2.1,2.2)$|\{p\}|$次.

2.1 从$\{p\}$中选择一个参数值$p_i(1 \leqslant i \leqslant |\{p\}|)$.

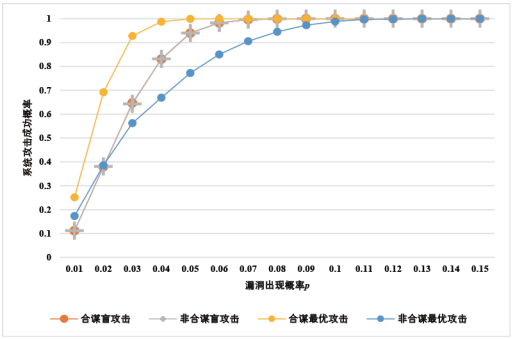
2.2 按步骤(2.2.1~2.2.3)进行H次实验.

2.2.1 生成异构执行体集合$E(i,j)(1 \leqslant j \leqslant H)$. 根据漏洞出现概率$p_i$,重复$\omega$次均匀分布实验生成一个$\omega$维0-1向量的执行体. 重复上述步骤生成$m$个异构组件得到执行体-漏洞矩阵.

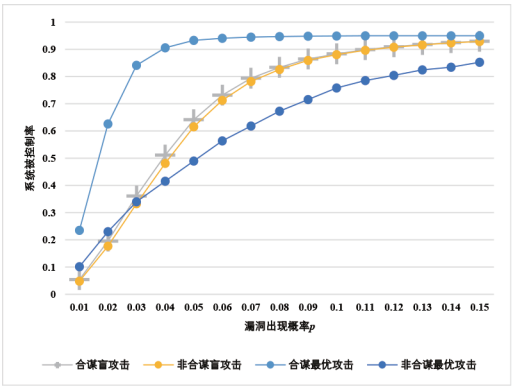
2.2.2 根据定义4生成服务体-漏洞矩阵.

2.2.3 计算四种攻击策略下的系统攻击成功率$\mathrm{SPr}(i,j)$和被控制率$\theta(i,j)$.

2.3 根据式$\mathrm{SPr}(i) = 1/H \times \sum_{j=1}^{H} \mathrm{SPr}(i,j)$和$\theta(i) = 1/H \times \sum_{j=1}^{H} \theta(i,j)$,得到$p_i$时的系统攻击成功率和被控制率.



(a)　p对系统攻击成功率的影响



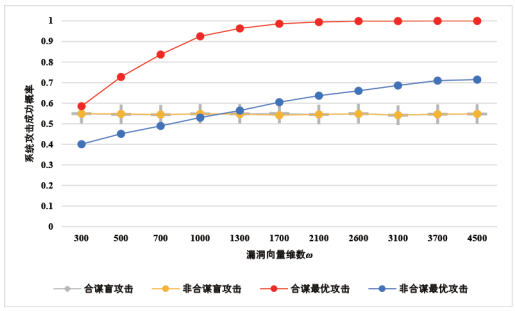
(b)　p对系统被控制率的影响

图2　p对系统攻击成功率及被控制率的影响

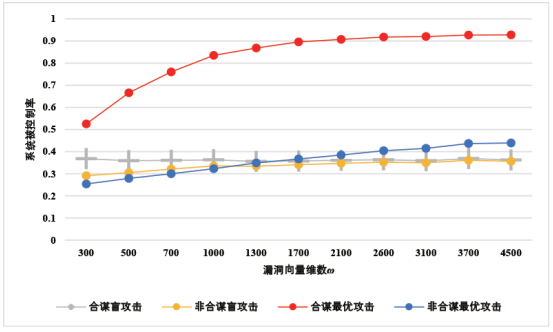
当p小于0.09时,减少漏洞显著降低了攻击成功率,这再次说明漏洞修补的必要性. 此外,从图2(b)可看出,相比其他策略,合谋最优攻击的系统被控制率增速更快,说明前期攻击时该策略的系统攻击成功率更高.

4.2　漏洞维数ω对系统安全性的影响

参数ω对系统安全性影响的实验设计与方案1类似. 相关参数设置为$p = 0.03, m = 30, n = 3, k = 2, N = 20, t_s/t_a = 20, H = 100000$. ω的取值范围$\{300, 500, 700, 1000, 1300, 1700, 2100, 2600, 3100, 3700, 4500\}$,对应漏洞数为9至135,覆盖了漏洞数从少到多的场景. 图3为实验结果.



(a)　ω对系统攻击成功率的影响



(b)　ω对系统被控制率的影响

图3　ω对系统攻击成功率与被控制率的影响

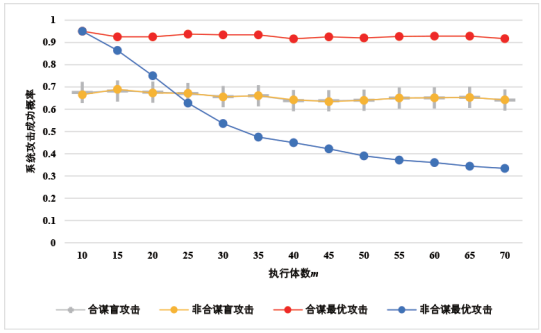
如图3所示,最优攻击时ω与系统安全性呈负相关;但盲攻击时ω与系统安全性未显示出相关性,且是否合谋对安全性影响不大. 其原因为:盲攻击时攻击者将遍历所有攻击序列A_τ,此时系统攻击成功率主要与$P_{\omega-\eta_i}^{\min(\omega-\eta_i,\tau_{\max})}/P_{\omega}^{\tau_{\max}}$的大小相关. 但本实验中$\omega$变化对该比值影响很小. 最优攻击时,因已知服务体-漏洞矩阵,此时攻击成功率主要与$|\mathrm{R}(\boldsymbol{M}_{S\text{-}V}, A^*_{\tau_{\max}})|$的大小相关,而$\omega$增大会导致$|\mathrm{R}(\boldsymbol{M}_{S\text{-}V}, A^*_{\tau_{\max}})|$显著增加,进而使攻击成功率增大.

4.3　执行体数m对系统安全性的影响

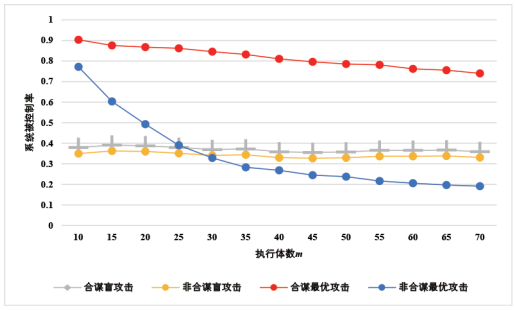
参数m对系统安全性影响的实验与方案1类似. 参数设置为$p = 0.03, \omega = 1000, n = 3, k = 2, N = 20, t_s/t_a = 20, H = 100000$. m的取值范围为$\{10, 11, \cdots, 70\}$. 实验结果如图4.

如图4所示,盲攻击时m对系统安全性没有明显影响;但最优攻击时m与系统安全性呈正相关. m决定了DHR系统中服务体数目,对DHR随机性起重要作用. 盲攻击时,服务体选择和攻击选择均随机. m对两者影响程度相当,此时m不会明显影响系统的安全性. 但最优攻击并不随机选择攻击,此时随机性可有效增强系统的安全性,特别在非合谋攻击时. 当合谋最优攻击且攻击者较多时,因每轮攻击覆盖的漏

洞数较多，故此时随机性也不会带来显著的安全性提升.



(a) m对系统攻击成功率的影响



(b) m对系统被控制率的影响

图4 m对系统攻击成功率及被控制率的影响

4.4 服务体模n和系统判决模k对系统安全性的影响

本文进行了单独改变服务体模n、单独改变判决模k和同时改变服务体模n及判决模k三种实验. n对系统安全性影响的方案设计如下.

方案2

1 给定参数$\{p,\omega,m,k,N,t_s/t_a\}$值和参数$\{n\}$.

2 重复步骤(2.1,2.2)H次.

2.1 生成异构执行体集合$E(i)(1\leqslant i\leqslant H)$. 根据漏洞出现概率$p$，利用均匀分布重复$\omega$次，生成一个$\omega$维0-1向量的执行体. 重复上述步骤生成$m$个异构功能组件得到执行体-漏洞矩阵.

2.2 重复步骤(2.2.1~2.2.3)$|\{n\}|$次.

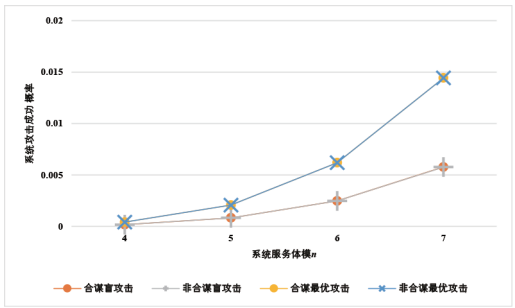
2.2.1 从$\{n\}$中选择一个参数值$n_j\left(1\leqslant j\leqslant|\{n\}|\right)$.

2.2.2 根据定义4生成服务体-漏洞矩阵.

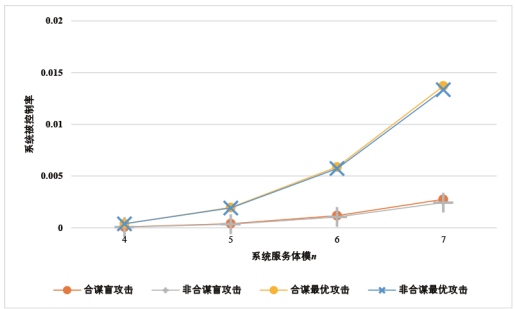
2.2.3 计算四种攻击策略的系统攻击成功率$\mathrm{SPr}(i,j)$和被控制率$\theta(i,j)$.

3 根据公式$\mathrm{SPr}(j)=1/H\times\sum_{i=1}^{H}\mathrm{SPr}(i,j)$和$\theta(j)=1/H\times\sum_{i=1}^{H}\theta(i,j)$，得到$n_j$时的系统攻击成功率和被控制率.

单独改变n的实验设置为$p=0.03,\omega=1000,m=30,k=4,N=20,t_s/t_a=20,H=100000$. n的取值范围为$\{4,5,6,7\}$. 单独改变k的实验设计与方案2类似. 设置为$H=100000$. k取值范围为$\{3,4,5\}$. 实验结果如图5、图6.

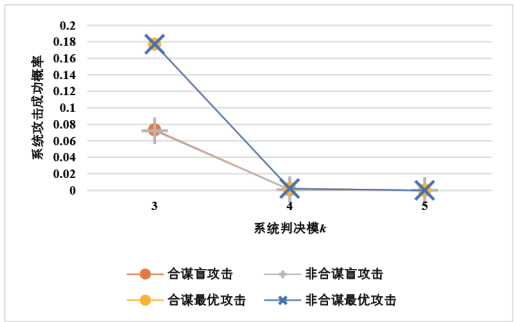


(a) n对系统攻击成功率的影响

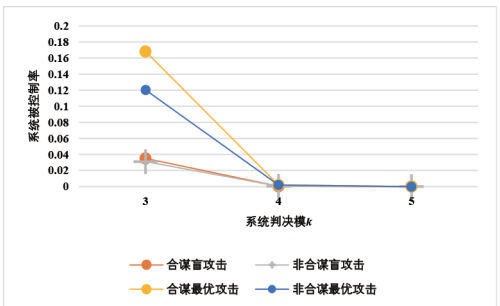


(b) n对系统被控制率的影响

图5 n对系统攻击成功率及被控制率的影响



(a) k对系统攻击成功率的影响



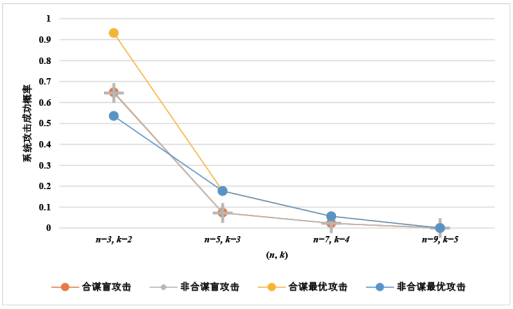
(b) k对系统被控制率的影响

图6 k对系统攻击成功率及被控制率的影响

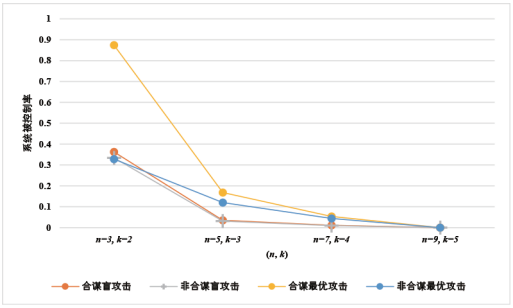
如图5、图6所示，判决模不变时服务体模与系统安全性呈负相关，服务体模不变时判决模与系统安全性呈正相关.

同时改变n和k的实验设置为$p=0.03,\omega=$

1000, m = 30, N = 20, t_s/t_a = 20, H =100000. n 的取值范围为{3, 5, 7, 9}, k 的取值为$(n+1)/2$. 实验结果如图7.



(a)　n、k对系统攻击成功率的影响



(b)　n、k对系统被控制率的影响

图7　n、k对系统攻击成功率及被控制率的影响

如图7所示,同时增大服务体模n和判决模k时系统的安全性会增加,结合图5和图6可知判决模k对系统的安全性影响要大于服务体模n.

4.5　攻击者数量N和系统调度周期与攻击时间比对系统安全性的影响

N对系统安全性影响的实验设计如下.

方案3

1　给定参数{$p, \omega, m, n, k, t_s/t_a$}值和参数{$N$}.

2　重复步骤(2.1~2.3) H次.

2.1　生成异构执行体集合$E(i)(1 \leqslant i \leqslant H)$. 根据漏洞出现概率$p$,利用均匀分布重复$\omega$次,生成一个$\omega$维0-1向量的执行体. 重复上述步骤得到$m$个异构功能组件,生成执行体-漏洞矩阵.

2.2　根据定义4生成服务体-漏洞矩阵.

2.3　重复步骤(2.3.1, 2.3.2)|{N}|次.

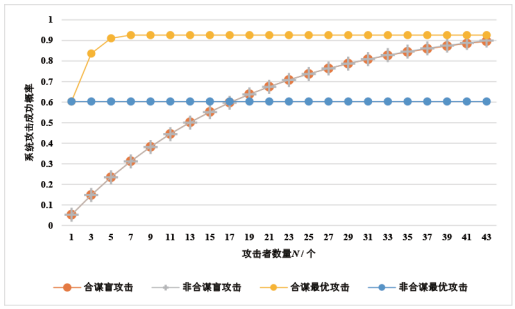
2.3.1　从{N}中选择一参数值$N_j(1 \leqslant j \leqslant |\{N\}|$.

2.3.2　计算四种攻击策略下的系统攻击成功率$\mathrm{SPr}(i,j)$和被控制率$\theta(i,j)$.

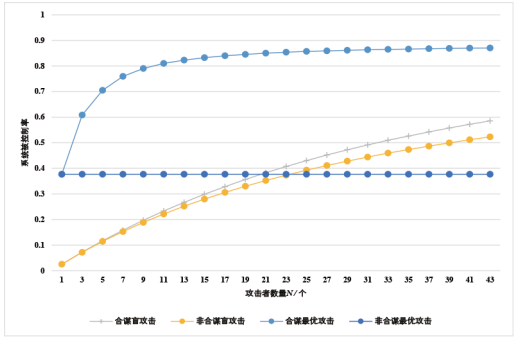
3　根据公式$\mathrm{SPr}(j) = 1/H \times \sum_{i=1}^{H} \mathrm{SPr}(i,j)$和$\theta(j) = 1/H \times \sum_{i=1}^{H} \theta(i,j)$,得到$N_j$时的系统攻击成功率和被控制率.

实验参数为p = 0.03, ω = 1000, m = 30, n = 3, k = 2, t_s/t_a = 20, H = 100000. N取值范围为{1, 3, …, 43}. 实验结果如图8.

从图8可看出,除了非合谋最优攻击外,其他攻击策略时N与系统安全性呈负相关. 非合谋最优攻击时攻击成功率不变是因为所有攻击者均使用相同攻击序列,等效于单人最优攻击. N大于20时,盲攻击的系统攻击成功率和被控制率均高于非合谋最优攻击. 这说明攻击次数较多时,盲攻击的效果也可能好于非合谋最优攻击.



(a)　N对系统攻击成功率的影响



(b)　N对系统被控制率的影响

图8　N对系统攻击成功率及被控制率的影响

t_s/t_a对系统安全性影响的实验方案设计与方案3类似. 参数设置为p = 0.03, ω =1000, m = 30, n = 3, k = 2, N = 20, H = 100000. t_s/t_a的取值范围为{1, 3, …, 39}. 实验结果如图9.

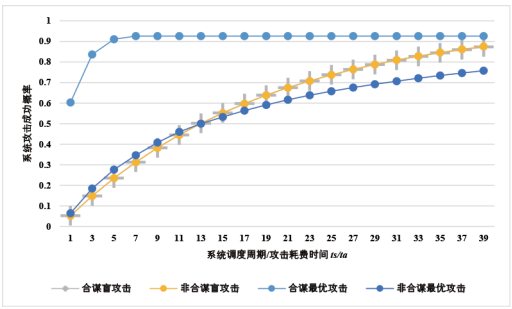
如图9所示,t_s/t_a与系统的安全性呈负相关. 调度周期t_s代表了DHR系统的动态性,t_s越小,系统动态性越高. 图9证实增加系统动态性可有效提高安全性.

4.6　讨论

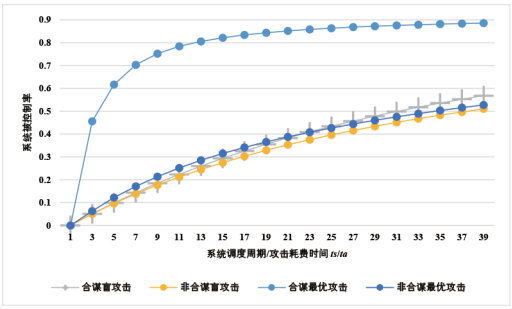
4.6.1　实验结果总结

上述实验结果表明,漏洞发生概率、漏洞维数、执行体数目、服务体模、判决模、攻击者数量、调度周期、攻击时间等因素对DHR系统的安全性均具有较大影响.

与黑盒模型相比,白盒模型时系统攻击成功率和被控制率更高. 但若各执行体中的漏洞过多,则无论白盒或黑盒模型,其系统安全性均很差. 减少执行体中的



(*a*) t_s/t_a与系统攻击成功率的影响



(*b*) t_s/t_a对系统被控制率的影响

图9 t_s/t_a对系统攻击成功率及被控制率的影响

漏洞,可有效提高系统的安全性,尤其在黑盒情况下.与黑盒模型不同,白盒模型时增加异构执行体数目可带来显著的安全性提高.判决模k是服务体漏洞筛除的决定性因素,故在系统安全性要求较高,且增加判决模带来的处理延迟较小时,可优先考虑增大判决模.

攻击者人数和调度时间与攻击时间之比对系统安全性都有明显的影响.但攻击者人数不仅影响攻击总次数,而且影响每轮的攻击次数,故攻击时增加攻击者数量更有效.

4.6.2 DHR系统增强建议

基于防御者角度,可改变的仅漏洞发生概率、漏洞维数、执行体数、服务体模、判决模、调度周期和隐藏系统内部实现细节等,综上,建议采取以下措施增强系统的安全性.

①适当增加执行体数目提高系统的随机性.增加执行体数目能有效提高系统随机性,进而提高系统的安全性.增加异构执行体通常会增加系统成本,尤其是执行体通过物理实体或虚拟机实现时.实践中可利用容器技术降低构建代价,同时提高执行体启动速度和降低清洗成本.

②适当增加系统判决模.增加判决模能有效筛除服务体中包含的漏洞,提高系统安全性,特别是判决模与服务体模相同时.实践中可根据安全态势动态调整系统判决模.安全态势严重时提高判决模,增加安全性.反之,降低判决模.

③减小系统调度时间.缩短调度时间能有效提高系统动态性,带来安全性提高,但调度时间过短也会带来较大的调度成本,因此需要研究有效的调度策略,在降低调度时间时不会增加过大成本.

④防止系统内部结构细节的泄漏.虽然DHR模型能显著提高系统的安全性,但黑盒时系统的安全性更高.因此,通过防止系统内部结构细节的泄露,使攻击者只能采用盲攻击策略,能有效提高系统安全性.在安全实践中,当系统检测到漏洞探测时,可通过随机返回错误响应迷惑攻击者.

⑤在调度算法中加入攻击感知响应.在当前服务体存在漏洞时,攻击者能通过暴力方法成功攻击系统.加入攻击失败次数限制,能有效缓解暴力攻击问题.如当系统检测到一定攻击后,就将当前服务体下线清洗.

⑥修补漏洞.当系统漏洞数目较多时,无论攻击者是否了解系统内部细节,其安全性都无法得到保障,因此需要将系统的漏洞数限制在一定范围.漏洞修补的具体方法可参考本文的最佳攻击序列构建算法.

以上措施中,②、④、⑥是首选,而③和⑤是现有DHR模型的改进方向.

4.6.3 与现有相关工作的对比

与现有基于概率分析方法[4,9]相比,本文所提出的方法不仅能完成单次攻击成功率计算,而且还可完成多攻击者合谋和非合谋情况下多次攻击的成功率及控制率计算,因而可更好地对系统安全性进行量化分析.

与基于自动机[5,6]和马尔可夫模型[7,8]的分析方法相比,本文所提方法先通过执行体-漏洞矩阵方法构建系统模型,然后进行安全性指标计算,所需专家人工操作较少.我们在拟态Web服务防御实践中,根据CVE漏洞库构建了漏洞矩阵模型,并通过漏洞测试对模型进行了验证.

此外,与其他安全性分析方法相比,本文的最优攻击序列选取算法还可用于DHR系统构建,修补最佳攻击序列对应的漏洞可取得最大安全增益.同时,本文给出了DHR模型各因素对系统安全性的影响,为DHR系统增强决策提供了量化数据支撑.

4.6.4 不足之处和后续研究展望

本文提出了一种基于概率分析的DHR模型安全性分析方法,推导了相关安全性指标的计算公式.从上述实验和分析可知,DHR模型比传统的防御技术具有更好的安全性.同时也可知,若选择的服务体中包含漏洞且调度周期较长时,理论上可通过协同攻击找出该服务体的漏洞.但因本文主要针对成功攻击一次的概率和对应的控制率进行分析,而实际攻击通常需要多步骤攻击多漏洞.此外,本文假设攻击者能力最大化,在模型中略去了漏洞探测验证、漏洞攻击难度及成本和攻击者能力大小等因素.这些假设会使计算的安全性

指标比实际要低. 虽然上述假设不会改变DHR模型的安全性比较结果和所提增强措施的正确性,但为了更好地度量DHR系统的安全性,后续研究中需充分考虑上述因素.

5 结语

本文针对DHR模型安全性量化问题进行研究,首先提出了执行体-漏洞矩阵、服务体-漏洞矩阵模型和它们的构建方法,用于表征DHR系统的内部结构和漏洞之间的关联. 随后,对四种攻击策略下的DHR系统攻击成功概率和被控制率计算公式进行了推导,并通过实验分析了不同策略下各因素对系统安全性的影响. 本文所提出的模型和安全性分析方法,能用于DHR系统和模型的安全性量化分析和比较,为DHR系统构建提供依据和参考. 后续,我们将对DHR模型改进、调度算法、考虑攻防成本和特定攻击偏好等因素的DHR模型安全性分析等工作开展进一步研究.

参考文献

[1] White House. Trustworthy cyberspace: strategic plan for the federal cyber security research and development program[R]. Report of the National Science and Technology Council, Executive Office of the President, 2011.

[2] 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.
Wu J X. Research on cyber mimic defense[J]. Journal of Cyber Security, 2016, 1(4): 1 – 10. (in Chinese)

[3] 王禛鹏, 扈红超, 程国振. 一种基于拟态安全防御的DNS框架设计[J]. 电子学报, 2017, 45(11): 2705 – 2714.
Wang Z P, Hu H C, Cheng G Z. A DNS architecture based on mimic security defense[J]. Acta Electronica Sinica, 2017, 45(11): 2705 – 2714. (in Chinese)

[4] 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.
Wang W, Zeng J J, Li G S, et al. Security analysis of dynamic heterogeneous redundant system[J]. Computer Engineering, 2018, 44(10): 42 – 45, 50. (in Chinese)

[5] 郭威, 邬江兴, 张帆, 等. 基于自动机理论的网络攻防模型与安全性能分析[J]. 信息安全学报, 2016, 1(4): 29 – 39.
Guo W, Wu J X, Zhang F, et al. A cyberspace attack and defense model with security performance analysis based on automata theory[J]. Journal of Cyber Security, 2016, 1(4):29 – 39. (in Chinese)

[6] 朱维军, 郭渊博, 黄伯虎. 动态异构冗余结构的拟态防御自动机模型[J]. 电子学报, 2019, 47(10): 2025 – 2031.
Zhu W J, Guo Y B, Huang B H. A mimic defense automaton model of dynamic heterogeneous redundancy structures[J]. Acta Electronica Sinica, 2019, 47(10): 2025 – 2031. (in Chinese)

[7] 任权, 贺磊, 邬江兴. 基于离散马尔可夫链的不同抗干扰系统模型分析[J]. 网络与信息安全学报, 2018, 4(4): 30 – 37.
Ren Q, He L, Wu J X. Analysis of different anti-interference system models based on discrete time Markov chain[J]. Chinese Journal of Network and Information Security, 2018, 4(4): 30 – 37. (in Chinese)

[8] 张兴明, 顾泽宇, 魏帅, 等. 拟态防御马尔可夫博弈模型及防御策略选择[J]. 通信学报, 2018, 39(10): 143 – 154.
Zhang X M, Gu Z Y, Wei S, et al. Markov game modeling of mimic defense and defense strategy determination[J]. Journal on Communications, 2018, 39(10): 143 – 154. (in Chinese)

[9] 李千目, 桑笑楠, 王仕豪, 等. 一种面向拟态防御架构的安全性分析方法[P]. 中国专利: CN110830462A. 2020-02-21.

[10] Zhang M Y, Wang L Y, Jajodia S, et al. Network diversity: A security metric for evaluating the resilience of networks against zero-day attacks[J]. IEEE Transactions on Information Forensics and Security, 2016, 11(5): 1071 – 1086.

[11] Miguel G, Bessani A, Neves N. Lazarus: Automatic management of diversity in BFT systems[A]. Proceedings of the 20th International Middleware Conference[C]. New York, USA: ACM, 2019. 241 – 254.

[12] Katerina G P, Wang F Y, Wang R, et al. Characterizing intrusion tolerant systems using a state transition model[A]. Proceedings DARPA Information Survivability Conference and Exposition II[C]. Anaheim, USA: IEEE, 2001. 211 – 221.

[13] Luo Z Y, Yang X, Sun G L, et al. Study of two kinds of analysis methods of intrusion tolerance system state transition model[J]. Review of Computer Engineering Studies, 2019, 6(1): 23 – 27.

[14] Miguel G, Bessani A N, Gashi I, et al. OS diversity for intrusion tolerance: Myth or reality?[A]. Proceedings of 2011 IEEE/IFIP 41st International Conference on Dependable Systems & Networks[C]. Hong Kong, China: IEEE, 2011. 383 – 394.

[15] Massimiliano A, Connell W, Venkatesan S, et al. Moving target defense quantification[A]. Adversarial and Uncertain Reasoning for Adaptive Cyber Defense[C]. Switzerland AG: Springer, 2019. 94 – 111.
[16] 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.
[17] Hong J B, Yusuf E S, Seong K D, et al. Dynamic security metrics for measuring the effectiveness of moving target defense techniques[J]. Computers & Security, 2018, 79:33 – 52.
[18] Ma D H, Wang L, Lei C, et al. Quantitative security assessment method based on entropy for moving target defense[A]. Proceedings of the 2017 ACM on Asia Conference on Computer and Communications Security [C]. New York, USA: ACM, 2017. 920 – 922.
[19] Hooman A, Jin B H, Julian J J, et al. Comprehensive security assessment of combined MTD techniques for the cloud[A]. Proceedings of the 5th ACM Workshop on Moving Target Defense[C]. New York, USA: ACM, 2018. 11 – 20.
[20] Brant A C, Corporation T M, Ziring N, et al. Common platform enumeration: Naming specification version 2.3 [R]. US Department of Commerce, NIST Inter-agency Report 7695, 2011.
[21] Quinlan J R. Induction of decision trees [J]. Machine Learning, 1986, 1(1): 81 – 106.

作者简介

郑秋华 男,1973 年 8 月出生,浙江杭州人.2007 年在浙江大学获工学博士学位.现为杭州电子科技大学网络空间安全学院讲师,主要研究方向为拟态安全、工控安全.

E-mail:zheng_qiuhua@163.com

申延召 男,1984 年 6 月出生,河南汝州人.2013 年在东华大学获得工学硕士学位,2018 年在山东大学获得理学博士学位.现为杭州电子科技大学网络空间安全学院讲师,主要研究方向为密码理论.

胡程楠 男,1996 年 8 月出生,浙江杭州人.2018 年在杭州电子科技大学获工学学士学位.现为杭州电子科技大学在读硕士研究生,主要研究方向为拟态安全、工控安全.

E-mail:chengnanhu@hdu.edu.cn

曾英佩 男,1984 年 6 月出生,浙江杭州人.2004 年和 2010 年在南京大学分别获得工学学士和工学博士学位.现为杭州电子科技大学网络空间安全学院副研究员,主要研究方向为软件安全.

崔婷婷 女,1990 年 4 月出生,山东青岛人.2012 年和 2018 年在山东大学分别获理学学士和理学博士学位.现为杭州电子科技大学网络空间安全学院讲师,主要研究方向为对称密码算法的分析和设计.

吴 铤(通信作者) 男,1972 年 10 月出生,浙江杭州人,2002 年在山东大学获理学博士学位.现为北京航空航天大学杭州创新研究院教授,博士生导师,主要研究方向为理论密码学、工控安全.

E-mail:wuting@hdu.edu.cn