

AMTD: 一种适应性移动目标防御方法

刘丹军, 蔡桂林, 王宝生

(国防科技大学计算机学院, 湖南 长沙 410005)

摘要: MTD 是通过动态移动目标的攻击面来改变攻击和防御不对称状态的一种新方式。MTD 变换频率对于系统可用性、安全性和防御成本之间的权衡至关重要。但目前的变换频率通常根据管理者的经验确定, 缺乏理论基础, 无法达到可用性—安全性成本之间的权衡。为应对这一挑战, 提出了适应性移动目标防御框架 (AMTD), 在确保系统可用的前提下, 以最低的成本获取最大的系统安全性。AMTD 的适应性体现在 2 方面: 一是防御模式的适应性, 通过提出一种自适应转换策略, 提供由安全警报触发的反应性防御和定时器到期事件触发的主动防御; 二是变换频率的适应性, 通过建立数学模型获得最优的变换频率。采取 4 个系列的模拟实验验证该解决方案的有效性。

关键词: 移动目标防御; 适应性防御; 框架

中图分类号: TP302

文献标识码: A

doi: 10.11959/j.issn.2096-109x.2018008

AMTD: a way of adaptive moving target defense

LIU Danjun, CAI Guilin, WANG Baosheng

Computer College, National University of Defense Technology, Changsha 410005, China

Abstract: Moving target defense is a new way to change the asymmetry state between attack and defense, by dynamically moving target's attacking surface. Frequency conversion of MTD is of great importance for the weighing between usability, security and defense cost. Nowadays, however, frequency conversion is usually determined by manager's experience, which cannot create a balance between usability and security cost for the lack of theory basis. An adaptive moving target defense framework (AMTD) was proposed. AMTD can maximize system security at the lowest cost while ensuring that the system is available. The adaptability of AMTD has two modes. Firstly, the defense mode, it contains an adaptive conversion strategy to provide reacting defense triggered by security alerts and active defense triggered by timer expiration events. The other mode is the frequency conversion, which obtain the optimal conversion frequency by establishing mathematical models. Four series of simulation experiments were taken to verify the effectiveness of the solution.

Key words: moving target defense, adaptive defense, framework

1 引言

随着互联网越来越成为全球各国发展的战略

性关键基础设施, 其安全问题的重要性越发突显。除了层出不穷的大规模网络攻击 (如 IP 前缀劫持^[1]、僵尸网络^[2]和 DDoS 攻击^[3]等), 近年来频繁曝出

收稿日期: 2017-11-29; 修回日期: 2018-01-04

通信作者: 刘丹军, liudanjun12@nudt.edu.cn

基金项目: 国家重点研发计划基金资助项目 (No.2017YFB0802301); 国家自然科学基金资助项目 (No.61472437)

Foundation Items: The National Key Research and Development Program of China (No.2017YFB0802301), The National Natural Science Foundation of China (No.61472437)

的重大安全事件（如“棱镜门”^[4]、心脏滴血（heartbleed）漏洞^[5]、WannaCry 勒索软件等）也都表明，网络空间易攻难守的安全局面对安全防护来说，始终是一个十分严峻的考验。

移动目标防御（MTD, moving target defense）^[6]是一种全新的防御理念，通过积极主动地改变目标状态，变换暴露在敌人面前的攻击面^[6~8]来削减攻击者有效发动攻击的能力。MTD 作为一种改变游戏规则变革性技术，有望从根本上改变当前网络“易攻难守”的局面，其一经提出即受到美国政府、国防部的重视。国内也受 MTD 思想影响，提出了基于拟态计算的拟态安全防护研究。

现有的移动目标防御机制方法^[6~8]中，攻击面变换频率通常依据管理者经验，缺乏理论基础，因此很难达到可用性—安全性—开销的平衡。对防御者来说，防御效果会受到变换频率的影响：目标攻击面变换越快，防御开销越大，但同时防御效果越好。然而，过于频繁的变换会导致系统性能下降甚至损害可用性^[9]；目标攻击面变换越慢，防御开销相应减少但同时防御效果会相对下降，系统被攻破的概率增大，一旦攻击成功，造成服务损失则得不偿失。因此，如何决定攻击面变换的时机、优化变换频率，获得可用性—安全性—开销的平衡，这是一个值得深入研究的重要方向。

本文提出了一个具有适应性的移动目标防御机制（AMTD, adaptive moving target defense）框架，期望能够以最小的时间开销获得最大的安全收益（系统安全性与系统可用性的综合体现），主要贡献有 2 方面。

1) 本文提出一种基于主动防御变换和反应式防御变换的适应性防御策略，通过防御方式和攻击面变换时间的适应性调整，实现 AMTD 框架。

2) 本文提出适应性目标移动变换的建模计算方法，包括变换的触发条件以及变换的时间间隔的优化求解，并通过实验模拟给出计算方法有效性验证。

2 相关工作

现有 MTD 攻击面变换通常采用 3 种策略：

预设固定时间间隔、使用可调时间间隔和异常事件驱动的变换^[10]。当前研究多是采用单一策略，而且前 2 种研究占多数。并且通常采用基于时间间隔（包括预设固定时间间隔和使用可调时间间隔）的变换策略，其中大部分时间触发机制是状态无关的^[11]，因此此类策略驱动下的攻击面变换往往缺乏针对性，没有做到可用性—安全性—开销优化平衡。第三种方式的机制（如 MOTAG）的防御效果完全依赖于检测机制的准确率和时效性，由于对异常事件的人为定义不一定准确和完善，且对异常事件进行检测可能会存在遗漏和延迟。另一些研究将第一种或第二种方式与第三种方式相结合，如 ChameleonSoft^[12]、TALENT^[13]、MAS^[14]。此类机制相对较少且主动防御频率与反应式防御频率是相互独立的，因此可能会出现在进行反应式防御过后的短时间内又实现主动式防御，虽然这一方式可以使系统所获得的安全度较高，但也存在一定的开销浪费。

在文献[15]和文献[6]中，作者都对最优变换频率问题进行了初步研究，期望在实现防御目标的同时减少不必要的开销和资源浪费/最小化系统性能的损失。确切地说，文献[15]期望能够求得最小变换频率从而降低开销和资源浪费。但实际上，该方法所利用的计算公式无法求得一个最优值，只能通过依据防御者所能接受的攻破概率来调整变换的间隔时长。文献[6]期望能够降低已部署众多虚假节点的网络中真实节点被识别的概率且同时最小化系统性能的损失，即网络服务的失效率。为此，作者设计了如下的最优 IP 随机化策略：若系统（真实节点）当前连接数为 0，则立即进行随机化；若攻击者的扫描速率足够低，那么等连接到真实节点的所有连接都完成再进行随机化，否则，立即进行随机化。但是，扫描概率足够低是一个模糊的概念，而且，若是重要服务，难以出现连接数为 0 的时刻。由上可知，针对系统的可用性—安全性—开销之间的均衡优化问题，目前还没有很好的解决方案。

3 适应性移动目标防御机制框架

3.1 AMTD 整体设计

AMTD 旨在根据目标系统的安全状态自适应

地变换攻击面,将主动防御与反应式防御相结合,有效降低系统安全风险。

本文将系统的安全状态建模为网络环境的安全状态和系统自身的安全状态。一方面,通过入侵检测系统(IDS, intrusion detection system)的预警信息来体现网络中是否出现异常事件,以标定网络环境安全性;另一方面针对系统自身的安全状态,本文认为即使在IDS没有预警的情况下,随着时间的推移,当前系统配置(即攻击面信息)潜在的安全风险在不断上升,通过计时器期满事件来标定系统本身的安全性。

AMTD的防御适应性主要采取两类策略。

1) 基于防御方式的适应性策略

AMTD目前采用2种适应性防御方式:一种是基于IDS的预警信息识别突发安全威胁,实现基于网络安全状态异常事件驱动的变换(ADS, anomaly-driven shuffling);另一种是基于系统风险递增的认知,采用基于计时器期满驱动的变换(TDS, timer-driven shuffling)。前者提供反应式防御,用于降低系统所遭受的损失,后者提供主动式防御,弥补入侵检测系统可能出现的漏报和误报所导致的不足,及时降低当前的潜在风险。

2) 基于变换间隔的适应性策略

TDS的变换间隔时长(τ)是依据2种输入信息计算:AMTD定义的时间窗(T_w)内所发生异常事件及攻击面变换历史信息,因此,从时间维度来看, τ 值是适应性变化的。

AMTD的工作原理如图1所示(服务器 S' 表示的是蜜罐系统/假目标,用于统计、记录攻击的信息)。在 t_1 时刻,AMTD接收到IDS发出的预警信息,MTD Manager会依据ADS的触发条件触发并成功实现ADS变换(t_2 时刻变换完成),目标系统的攻击面发生变化,导致当前预警信息所指示的攻击失效,从而实现对目标系统的及时保护。但是由于IDS的准确率无法达到100%,假如没有报警,目标系统的潜在安全风险不断上升,当累积到一定程度时会发生计时器期满事件(t_3 时刻),从而触发并执行TDS变换(t_4 时刻变换完成),以降低因IDS误报和漏报所导致的威胁。每一次具体的ADS变换和TDS变换方法可以是软件变换技术、动态平台技术、网络地址变换技术当中的某一种。在现阶段,只考虑在整个AMTD运行过程中仅采用某一种具体的网络地址变换技术,如RPAH^[16]。

AMTD系统框架的结构组成如图2所示。该系统一共包括4个单元:MTD防御管理单元、条件检测器、异常反应式变换单元ADS和计时器驱动式变换单元TDS。

1) MTD防御管理单元主要负责2个功能。

① 针对当前系统的安全状态,决定是否触发攻击面的变换,具体来说实现以下2种决策:

a) 接收从入侵检测系统发送过来的预警信息,并决定是否进行基于异常事件驱动的ADS变换,若决定进行变换,那么触发ADS单元实现

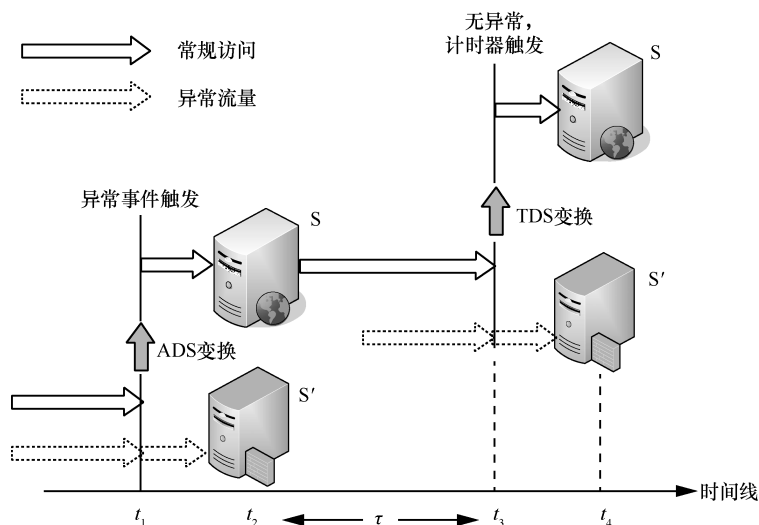


图1 AMTD工作原理示意图

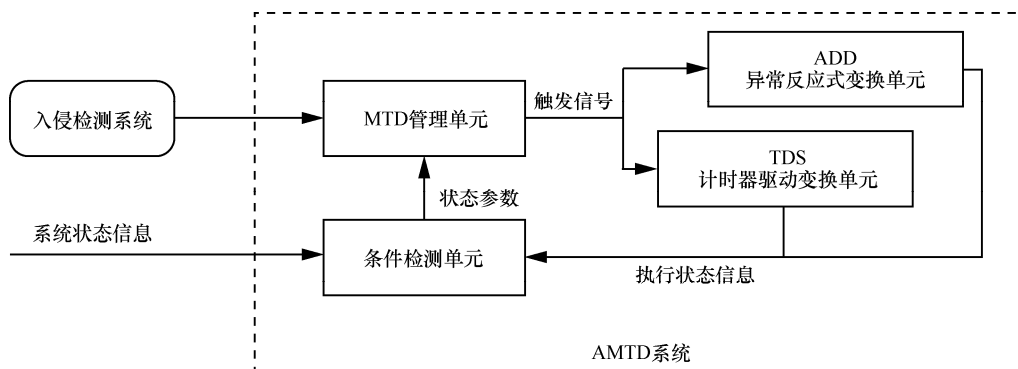


图2 AMTD 框架结构组成示意

ADS 变换的发生;

b) 当发生计时器期满事件的时候,触发 TDS 单元实现 TDS 变换的发生。

② 依据该系统框架所定义的时间窗内系统安全状态的变化历史,来优化攻击面变换的触发条件。 T_w 是一个滑动时间窗参数,由系统确定。

2) 条件检测器主要监测并收集以下 3 类状态信息。

① 系统自身的状态信息(system state),包括系统被攻破后恢复可用性所需的开销, T_w 内入侵事件的平均到达间隔, T_w 内入侵检测的查准率(precision)和查全率(recall)^[17]。

② ADS 单元的执行状态信息(ADS-execution state),包括在 T_w 内所完成 ADS 变换的变换开销集合、当前 ADS 变换完成的时间值。

③ TDS 单元的执行状态信息(TDS-execution state),包括当前 TDS 变换的完成情况、当前 TDS 变换完成的时间点。

3) ADS 单元的主要功能包括:

① 执行 ADS 变换;

② 将 ADS 执行状态(此次变换的完成情况,包括开销和完成时间)发送给 Condition Monitor。

4) TDS 单元的主要功能包括:

① 执行 TDS 变换;

② 将 TDS 执行状态(此次变换的完成情况,包括开销和完成时间)发送给 Condition Monitor。

3.2 适应性变换策略

本节围绕适应性目标移动变换的建模和适应性变换策略设计展开,首先建立一个数学模型来分析 AMTD 框架下 TDS 变换和 ADS 变换 2 种变换策略所引入的开销和带来的收益,包括计算

ADS 变换的触发条件以及 TDS 变换的最优时间间隔(TDS 变换的触发条件即为所求得的最优时间间隔)。

3.2.1 AMTD 系统模型

假设被保护目标系统是一个企业网络的内部服务器,攻击者针对目标系统的入侵事件到达间隔时间服从参数为 μ 的指数分布[6,15](在实际使用中, μ 值可依据 T_w 时间内的攻击历史统计得来),即 $I(t) = 1 - e^{-\frac{t}{\mu}}$ 。其中, $I(t)$ 表示在 $[0, t]$ 内攻击者针对目标系统的入侵事件到达间隔所服从的概率分布。

本文提出一个量化指标——系统服务率 ξ ,来量化一个 MTD 系统正常运行所引入的开销对用户正常获取服务所带来的影响。 ξ 代表系统正常对用户提供服务时间占其运行总时间的比率,记为

$$\xi = \frac{\text{系统对外提供服务时间}}{\text{系统运行总时间}} \quad (1)$$

若将 $[0, t]$ 时间间隔内服务器正常为用户提供服务时间的数学期望记为 $E(t)$,则 $E(t)$ 可表示为

$$E(t) = t - \sigma(t) - \gamma(t) - \delta(t) \quad (2)$$

其中, $\sigma(t)$ 表示在 $[0, t]$ 时间间隔内进行的 TDS 变换所产生开销的数学期望, $\gamma(t)$ 表示在 $[0, t]$ 时间间隔内进行的 ADS 变换所产生开销的数学期望,用 $\delta(t)$ 表示系统恢复可用性所需要的时间数学期望,代表被侵入损失。

在时间 t 趋于无穷大的情况下,式(1)所表示的服务率又可表示为

$$\xi = \lim_{t \rightarrow \infty} \frac{E(t)}{t} = 1 - \frac{\sigma(t) + \gamma(t) + \delta(t)}{t} \quad (3)$$

式(3)从数学角度描述了当系统处于稳定状态时的对外服务率。

3.2.2 AMTD 变换策略

AMTD 机制运行的目标是在保证系统安全性的前提下, 目标系统对外服务率最大化。首先分析 ADS 开销 $\gamma(t)$ 、被侵入损失 $\delta(t)$ 和 TDS 开销 $\sigma(t)$ 的计算依据, 并据此制定适应性变换策略, 包括 ADS 变换的触发条件, 以及 TDS 的变换间隔。

1) ADS 开销 $\gamma(t)$

假设前一次执行变换 (TDS 变换或 ADS 变换) 的时刻为 t_0 , 经过了 t_a 时间, IDS 发出攻击报警, 假设系统发出预警的时刻至攻击到达最终窃取信息阶段之间的时间差为 t_{lead} , 在 t_{lead} 时间内 AMTD 系统可采取 ADS 变换提供反应式防御从而保证系统 S 不受侵害。

同时, 在 S 原先位置上部署蜜罐/假目标 S', 以监测和统计攻击信息 (具体设计可参见 NMC^[18])。

t_{lead} 为随机时间, 通常为数秒到数分钟^[18], 本文假设 t_{lead} 的值服从指数分布^[19], 其概率分布函数记为 $L(t)$ 。

当入侵检测报警为 TP (true positive) 时, 此次 ADS 变换被认为系统提供有效的防御, 定义预警是否正确的标准如下。

- ① 对于蜜罐目标 S', 若在入侵报警后缺失被攻击, 即在时间范围 $[t_0+t_a, t_0+t_a+t_{lead}]$ 内 (如图 3 所示) 发生入侵, 则认为 IDS 报警正确。
- ② 若时间范围 $[t_0+t_a, t_0+t_a+t_{lead}]$ 内蜜罐系统无入侵迹象, 则认为 IDS 报警为误报。
- ③ 若蜜罐系统入侵时间大于 $[t_0+t_a+t_{lead}]$, 则认为 IDS 为漏报。

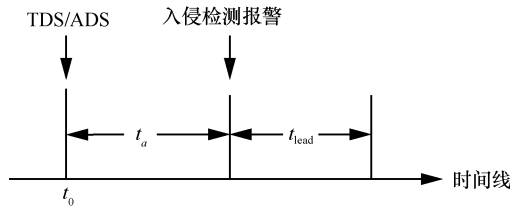


图3 ADS 机制运行所涉及时间图样

因此, AMTD 系统在接收到 IDS 的预警信息之后, ADS 变换单元会首先判断是否需要触发 ADS 变换, 以减小因误报导致多余开销。本文的判断依据是当前系统忽略报警之后被攻击损失开销期望 O_{nads} 大于执行 ADS 变换开销期望 O_{ads} 时,

进行 ADS 变换, ADS 变换的触发条件可表示为

$$O_{ads} \leq O_{nads} \quad (4)$$

具体来说, 可以计算接收到入侵检测预警后即执行 ADS 变换所产生开销的数学期望 O_{ads} 为

$$O_{ads} = pc_1 + \bar{p}c_1 = c_1 \quad (5)$$

其中, p 为 IDS 的准确率, c_1 为单次 ADS 变换开销。接收到预警信息后对其忽略不进行 ADS 变换的时间开销的数学期望 O_{nads} 为

$$O_{nads} = pc_3 \quad (6)$$

其中, c_3 为一次入侵成功后对系统带来的时间损失。

综合式(4)~式(6)计算得

$$c_1 \leq pc_3 \quad (7)$$

因此是否进行 ADS 变换取决于 3 个因素: 单次 ADS 变换开销 c_1 、入侵检测查准率 p 以及系统被攻破后到恢复正常的可用性所遭受的时间损失 c_3 。

此外, 当决定执行 ADS 变换时, 只有具有足够的提前时间 t_{lead} , 才能保证一次 ADS 变换顺利完成。用 m 表示 ADS 变换成功完成的概率, 则有 $m = \overline{L(c_1)} = 1 - L(c_1)$, 其中 $L(t)$ 是 t_{lead} 的概率分布。设 q 表示是否执行 ADS 变换, 则

$$q = \begin{cases} 1, & c_1 \leq pc_3 \\ 0, & c_1 > pc_3 \end{cases} \quad (8)$$

那么, 一次 ADS 可顺利完成的概率为 mq 。

基于上述分析与假设, 对时间间隔 $[0, t]$ 内 ADS 变换开销的数学期望进行如下分析。

假设在时间间隔 $[0, t]$ 内 IDS 发出的警报数为 $n_{alert}(t)$, 入侵检测的查全率为 r (recall)。同时, μ 为本节所提到的入侵事件的平均到达间隔时间, 则在 $[0, t]$ 时间间隔内攻击者入侵次数的期望值为 $\frac{t}{\mu}$ 。那么, 在 $[0, t]$ 时间间隔内的 TP (true positive)

预警数量为 $\frac{rt}{\mu}$, 记为 $n_{positive} = \frac{rt}{\mu}$ 。由于 $n_{positive} =$

$pn_{alert}(t)$, 则 $n_{alert}(t) = \frac{rt}{p\mu}$ 。此外, 由上可知, 一次

ADS 变换成功完成的概率为 mq 。因此, 在 $[0, t]$ 间隔内依据 IDS 预警成功完成的 ADS 变换的数量为 $mqn_{alert}(t) = \frac{mqrt}{p\mu}$ 。又由于单次执行 ADS 变

换的开销为 c_1 , 因此可以得到 $[0, t]$ 内 ADS 变换开

销的期望为

$$\gamma(t) = \frac{e_1 m q r t}{p \mu} \quad (9)$$

2) 被侵入损失 $\delta(t)$

本文用系统恢复可用性所需要的时间表示目标系统的被侵入损失。具体损失包括以下 3 类原因。

① 漏报导致

在 $[0, t]$ 时间间隔内, 未探测到的入侵数量为 $\bar{r} \frac{t}{\mu}$, 其中, r 为查全率 (recall) 且 $\bar{r} = 1 - r$, 由于目标服务器被成功攻破一次所遭受的损失为 c_3 , 那么在 $[0, t]$ 时间间隔内, 因未探测到入侵导致系统被攻破的损失为 $\frac{\bar{r} t}{\mu} c_3$ 。

② t_{lead} 较短导致

在这种情况下, 虽然 IDS 已经正确检测到入侵并发出了预警, 但是 t_{lead} 太短不足以完成 ADS 变换, 导致系统被攻破从而带来被侵入损失。

$m r \frac{t}{\mu}$ 为已正确探测到攻击并预警, 但由于 t_{lead} 小于 c_1 从而没有成功完成 ADS 变换导致系统被入侵次数的数学期望 (其中 $m = 1 - m$), 且由于目标服务器被成功攻破一次所遭受的损失为 c_3 , 那么在 $[0, t]$ 时间间隔内, 因 t_{lead} 较短导致系统被攻破所带来的被侵入损失为 $\frac{\bar{m} r t}{\mu} c_3$ 。

③ IDS 正确警报, 但 AMTD 系统忽略报警导致

在 $[0, t]$ 间隔内, 入侵检测发出正确的入侵报警, 同时具有足够的 t_{lead} , 但 AMTD 做出忽略报警的决策次数的数学期望为 $\bar{q} m r \frac{t}{\mu}$ (其中 $\bar{q} = 1 - q$), 且由于目标服务器被成功攻破一次所遭受的损失为 c_3 , 那么在 $[0, t]$ 时间间隔内, 当 IDS 正确探测到入侵并预警, 但 AMTD 忽略报警未触发 ADS 变换从而导致系统被攻破的被侵入损失为 $\frac{\bar{q} m r t}{\mu} c_3$ 。

另一方面, 为降低上述 ADS 变换时目标系统可能面对的被入侵风险, AMTD 采用 TDS 变换机制来弥补 ADS 机制的不足。设 2 次变换间隔时长为 τ , 并用 n 表示 TDS 变换成功的概率。那么在 $[0, t]$ 时间间隔内, 因执行 TDS 变换而避免的被侵入损失的数学期望值应为

$$\frac{\bar{t} r + c \bar{m} r + t m r \bar{q}}{\mu} n c_3$$

因此, 在 $[0, t]$ 时间间隔内的被侵入损失的数学期望可表示为

$$\begin{aligned} \delta(t) &= \frac{\bar{t} r}{\mu} c_3 + \frac{\bar{t} m r}{\mu} c_3 + \frac{t m r \bar{q}}{\mu} c_3 - \frac{\bar{t} r + c \bar{m} r + t m r \bar{q}}{\mu} c_3 \\ &= \frac{(1 - m r q)(1 - n) t c_3}{\mu} \end{aligned} \quad (10)$$

TDS 变换成功的概率即为 2 次入侵之间的时间间隔时长大于 TDS 变换间隔 τ 的概率, 根据本节起始处的假设, $I(t)$ 表示的是在 $[0, t]$ 内攻击者对目标服务器的入侵事件到达间隔所服从的概率分布, 则有 $n = \overline{I(\tau)} = 1 - I(\tau) = e^{-\frac{\tau}{\mu}}$ 。

因此, 式(10)所表示的 $[0, t]$ 时间间隔内的被侵入损失的数学期望又可表示为

$$\delta(t) = \frac{(1 - m r q)(1 - e^{-\frac{\tau}{\mu}}) t c_3}{\mu} \quad (11)$$

3) TDS 开销 $\delta(t)$

TDS 计时器事件驱动发生的变换采用可调时长间隔的变换, 当间隔时长达到 τ 时, 即触发 TDS 变换。上面已经分析了单次 TDS 变换成功的概率为 $n = e^{-\frac{\tau}{\mu}}$, 那么在任意 2 个入侵事件发生的时间间隔内, 能够完成 TDS 变换次数的数学期望为

$$\begin{aligned} N_{\text{TDS}} &= e^{-\frac{\tau}{\mu}} + e^{-\frac{2\tau}{\mu}} + e^{-\frac{3\tau}{\mu}} + \dots + e^{-\frac{j\tau}{\mu}} + \dots \\ &= \sum_{j=1}^{\infty} e^{-\frac{j\tau}{\mu}} \\ e^{-\frac{\tau}{\mu}} N_{\text{TDS}} + e^{-\frac{\tau}{\mu}} &= \sum_{j=1}^{\infty} e^{-(j+1)\frac{\tau}{\mu}} + e^{-\frac{\tau}{\mu}} = N_{\text{TDS}} \end{aligned}$$

因此得到

$$N_{\text{TDS}} = \frac{e^{-\frac{\tau}{\mu}}}{1 - e^{-\frac{\tau}{\mu}}} \quad (12)$$

假设单次实施 TDS 变换的开销为 c_2 , 那么在 $[0, t]$ 时间间隔内, 执行 TDS 变换所引入开销的数学期望可以表示为

$$\sigma(t) = \frac{t}{\mu} \frac{e^{-\frac{\tau}{\mu}}}{1 - e^{-\frac{\tau}{\mu}}} c_2 \quad (13)$$

由式(3)、式(6)~式(12), 得服务率为如下形式。

$$\xi = 1 - \frac{mqr}{p\mu} c_1 - \frac{1}{\mu} \frac{e^{-\frac{\tau}{\mu}}}{1 - e^{-\frac{\tau}{\mu}}} c_2 - \frac{(1 - mrq)(1 - e^{-\frac{\tau}{\mu}})}{\mu} c_3 \quad (14)$$

对 ξ 求极值, 即对式(14)关于自变量 τ 求一阶导数并使其值为 0, 从而求得最优的 TDS 变换间隔为

$$\tau^* = -\mu \ln \left(1 - \sqrt{\frac{c_2}{(1 - mrq)c_3}} \right) \quad (15)$$

再根据式(7)将 q 按照实际取值代入式(15)后可得

$$\tau^* = \begin{cases} -\mu \ln \left(1 - \sqrt{\frac{c_2}{(1 - mr)c_3}} \right), & c_1 \leq pc_3 \\ -\mu \ln \left(1 - \sqrt{\frac{c_2}{c_3}} \right), & c_1 \geq pc_3 \end{cases} \quad (16)$$

当 $\tau = \tau^*$ 时, ξ 取得最大值。

4 模拟验证

为了测试 AMTD 机制是否可靠, 本文开发了 AMTDSim 模拟器。该模拟器的驱动方式是基于事件的, 事件分为异常事件和计时器满事件, AMTDSim 能够基于系统被攻击事件 trace 或自定义参数(如表 1 中的参数)模拟真实网络系统中受到的攻击事件和 MTD 变换事件, 从而有效测试 AMTD 机制的可靠性并评估网络系统的可用性。其中, 攻击事件 trace 既可以是导入的现实存在的攻击事件, 也可以是自定义的攻击事件。在本文中, 考虑到网络系统可能受到密集程度不同的攻击, 为了验证 AMTD 机制对此的适应性, 模拟生成了 2 个攻击事件的 trace(都符合指数分布, 且攻击事件发生的时间间隔的均值 μ 为 24 h 的 trace1 和 3 h 的 trace2)。另外, 依据现实情况, 可认为一次 MTD 变换的发生, 会对之后 $t_{\text{effective}}$ 时间内的攻击事件起到阻止作用, 本实验过程根据文献[20]中的记录数据, 设置 MTD 变换有效系数 $\phi=0.05$, 表示将不处理 MTD 变换后 0.05μ 时间内发生的攻击事件。

考虑到 IDS 的预警会有漏报和误报, 而本实验中生成的攻击事件 trace 并不能体现这一点, 所以 AMTDSim 需要根据 IDS 的 2 个参数(precision 和 recall)改进攻击事件的分布(正确预警、漏报

和误报), 以模拟真实网络系统的环境。改进过程是, 首先计算 IDS 的正确预警数、漏报数和误报数, 根据正确预警数和误报数对攻击事件 trace 进行标记, 并把漏报事件随机插入攻击 trace 中。令 N_{event} 为总攻击事件数, N_{allalarm} 为总预警数, N_{actual} 为预警正确的攻击事件数, $N_{\text{erroralarm}}$ 为误报数。易知 $N_{\text{allalarm}} = N_{\text{erroralarm}} + N_{\text{actual}}$, $N_{\text{actual}} = N_{\text{event}} \cdot \text{precision}$, 可得 $N_{\text{erroralarm}} = N_{\text{actual}} \left(\frac{1}{\text{precision}} - 1 \right)$ 。

进行实验时, 本文用系统的服务率(service rate)表示系统的可用性, 方法是, 记录实验过程中 MTD 变换(包括 TDS 变换和 ADS 变换)的总开销和系统受到攻击的总损失, 计算系统服务率 ξ , 之后的实验都和 ξ 值相关。根据式(3)可知, 防御的开销越小, 系统的服务率越高, 反之亦然。

AMTDSim 的自定义参数及其含义见表 1, 在进行实验时, 这些参数的取值范围依据相关研究和实际经验获得, 为提高实验准确性, 在参数范围内多次取不同值, 观察不同参数对系统服务率的影响。该实验假定 t_{lead} 的值服从指数分布, 把 t_{lead} 的均值记作 ω 。

表 1 模拟实验中所需设置的参数及其含义

参数	含义
p	IDS 系统的查准率
r	IDS 系统的查全率
C_{ADS}	单次实施 ADS 变换所需开销, 计量单位为秒
C_{TDS}	单次实施 TDS 变换所需开销, 计量单位为秒
C_{Loss}	系统被攻破后恢复可用性所需开销, 计量单位为秒
ω	IDS 预警到入侵事件到达之间的时间长度的均值, 计量单位为秒
T_{sim}	单次实验所模拟的现实时间中的时长

基于 AMTDSim 模拟器, 本文针对 4 个问题进行了 4 个实验: 1) 对比使用 AMTD 机制和使用固定时间间隔变换机制的系统服务率; 2) IDS 的检测精度对采用 AMTD 机制的系统服务率的影响; 3) 单次变换开销和被侵入损失的变化对系统服务率的影响; 4) IDS 预警提前量的变化对采用 AMTD 机制的系统服务率的影响。为减小实验的偶然性和误差, 对应数据下的每个实验都进行 30 次, 再取平均值作为实验结果, 且每一次实验的开始时间都是随机选择的(注意, 模拟的 2 个攻击 trace 的时间跨度是 3 年, 每次的独立实验起

始时间是前两年, 以确保每次实验模拟时长 T_{sim} 为 1 年)。

4.1 不同机制间服务率的比较

本实验对比采用 AMTD 机制和采用固定时间间隔变换的 MTD 机制(下文称基准 MTD 机制)时的系统服务率, 以说明采用 AMTD 机制时的系统服务率更高。本实验对 AMTD 机制的参数设置见表 2。

表 2 4.1 节实验的 AMTD 参数设置

参数	trace1	trace2
$\mu(\text{s})$	85 716(≈ 24 h)	10 819(≈ 3 h)
p	0.7	0.7
r	0.7	0.7
$C_{\text{ADS}}(\text{s})$	20	20
$C_{\text{TDS}}(\text{s})$	20	20
$C_{\text{Loss}}(\text{s})$	800	800
$\omega(\text{s})$	60	60
T_{sim}	1 Year	1 Year

进行实验时, 为了确保实验的可靠性, 需要探索到基准 MTD 机制的最优服务率, 用基准 MTD 机制的最优服务率和 AMTD 机制进行对比

才更有说服力。方法是, 在攻击 trace1 中, 先把基准 MTD 的初始变换间隔设置为 1 000 s (攻击 trace2 中设置为 300 s), 求得初始变换间隔下基准 MTD 的系统服务率(注意实验进行 30 次, 结果取平均值); 之后, 变换时间间隔每次递增 100 s, 并根据实验求得当前间隔下基准 MTD 机制的系统服务率; 最后将实验结果绘制成图 4 中曲线。而采用 AMTD 机制的系统服务率(定值)用虚线条体现。

从图 4 可看到, 基于攻击 trace1 和 trace2 的实验中, 基准 MTD 机制的系统服务率先是快速增长到达峰值而后不断下降直至平稳。分析结果如下。初始阶段, 变换时间间隔较短, 基准 MTD 进行高频变换, 有效抵御了攻击事件; 当变换间隔不断增大, 虽然变换频率降低了, 但更接近于攻击频率, 所以仍能抵御攻击, 结果是系统服务率增大, 直到抵达峰值; 之后, 随着变换间隔增大, 系统被攻破次数增多, 而节省下来的 MTD 变换开销不足以弥补系统被攻击导致的损失, 因而服务率不断下降。对比图 4(a)和 4(b)可知, 攻击事件越频繁, 系统服务率变化越明显, 最终达到一个服务率较低的稳态, 说明基准 MTD 机制不灵活, 不能有效权衡变换开销和攻击损失, 最

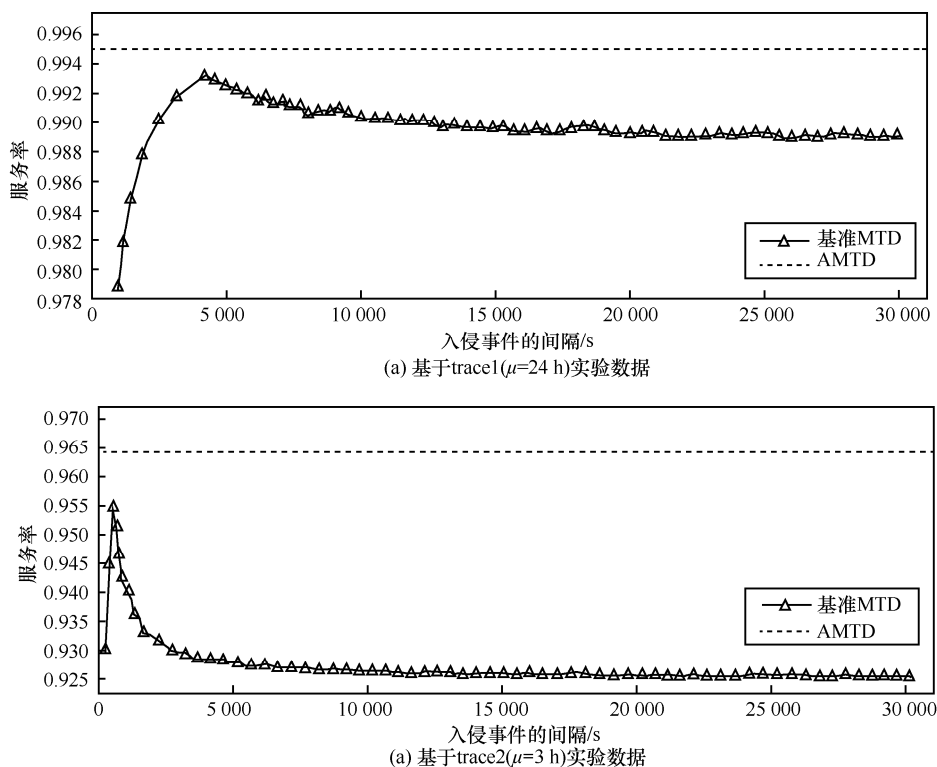


图 4 部署 AMTD 机制与基准 MTD 机制的服务率比较

后影响到系统的服务率。

对比图4中表示基于AMTD机制的系统服务率的虚线条和基于基准MTD机制的曲线条,虚线条对应的系统服务率始终高于曲线条的服务率峰值(现实环境中,攻击事件更灵活多变,基准MTD的服务率一般低于这个峰值),证明采用AMTD机制的系统比采用基准MTD机制的系统具有更高的系统服务率。这是由于在运行时,AMTD机制可根据攻击事件等系统自身的环境状态,调整MTD变换的时机,以获得较高的系统服务率。当 $precision=recall=0.7$ 时,在攻击trace1中,此时攻击密度较小,AMTD机制比基础MTD机制的服务率高0.2%;在trace2中,此时攻击密度较大,AMTD机制比基础MTD机制的服务率高1.1%。

此外,对比图4(a)和4(b)中采用AMTD机制的线条可发现,若攻击事件的密度增大,采用AMTD机制的服务率会下降。这是因为攻击密度增大,导致MTD变换次数增多,总的变换开销增加,提供正常服务的时间就会变短,这和现实世界的规律是吻合的。

4.2 入侵检测机制精度对服务率的影响

入侵检测的精度(p 和 r 值)也会对AMTD机制提供的服务率造成影响。若入侵检测的精度高,则AMTD的作用明显,系统的可用性也就高。本实验通过设置不同的IDS精度,观察对采用AMTD机制的系统服务率的影响,参数设置除了 p 和 r 值,其他值和表2参数值一样。

图5(a)和5(b)(彩图见插页1)对应IDS的 p 和 r 在取值范围 $\{0.1, 0.2, 0.3, \dots, 0.9\}$ 内,基于攻击trace1和攻击trace2采用AMTD机制的系统服务率的结果。尽管trace1和trace2的攻击密度不同,导致提供的系统服务率不同,但还是具有一定的相似性。从图5(a)和5(b)中可清楚地发现,IDS系统精度越高,系统服务率越高。另外发现一个规律,当查全率 $r > 0.4$ 时,采用AMTD机制的系统服务率会比采用基准MTD机制的服务率的峰值更高(基准MTD机制的服务率见图4);当 $p=r=0.9$ 时,在攻击trace1中,采用AMTD机制的服务率达到峰值99.63%,而在攻击trace2中,峰值是97.28%。显而易见,IDS精度越高,采用AMTD机制的系统服务率更高。

另外,还发现,采用AMTD机制的系统服务

率对查全率 r 更敏感,系统服务率会随着 r 值的增大而增大,即使 p 值处于一个较低值,只要 r 值较高,系统服务率仍能保持较高的值(见图5(a)和5(b));反之,若 r 值较低,无论 p 值多高,系统服务率还是会受到约束。仔细分析一下,本实验中 C_{ADS} 和 C_{TDS} 的值相对 C_{Loss} 的值来说较小,如果此时查全率 r 值很小,则IDS会漏报很多攻击事件,造成更大的系统损失。如果查准率 p 值很小,尽管IDS误报会很多,但是总的变换开销并不大(若ADS变换次数增多,则TDS变换次数相应减少),对系统服务率的影响不大。所以,本实验得出一个启示,如果想通过改善IDS的检测效率来提高系统服务率,提高 r 值要比提高 p 值更为关键。

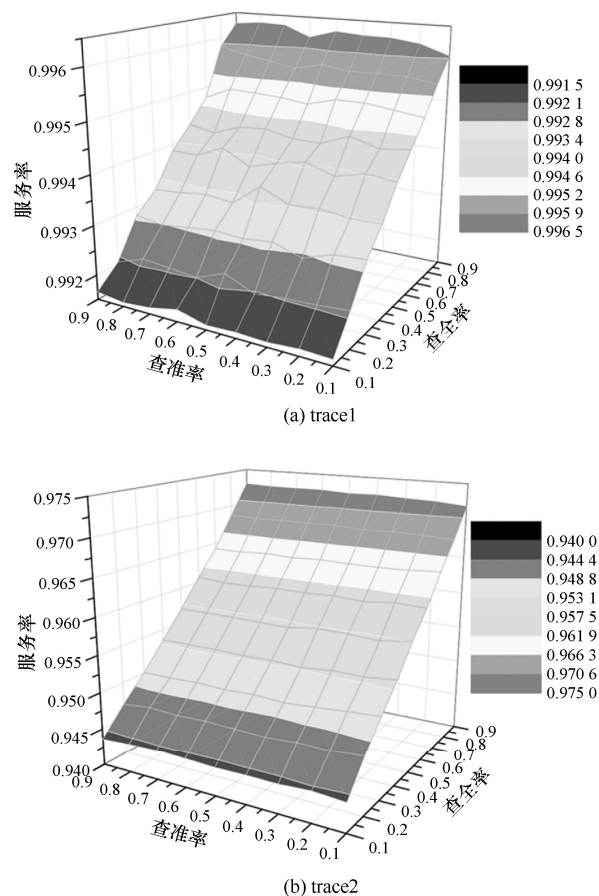


图5 入侵检测精度对系统服务率的影响

4.3 变换开销和被侵入损失变化对服务率的影响

本实验关注的问题是,变换开销(C_{ADS} 和 C_{TDS})与被攻击损失(C_{Loss})的比率对采用AMTD机制的系统服务率的影响。参数设置除了 C_{Loss} 值,其他值和表2中参数值一样。

由于本实验结果与 ADS 和 TDS 变换的行为差异无关,所以暂时只考虑一种变换机制,即假定 ADS 和 TDS 变换的行为相同,即 $C_{ADS}=C_{TDS}$,并简称为 MTD 变换开销。进行实验时,可保持 MTD 变换开销值为 20 s 不变,仅通过改变 C_{Loss} 的值间接改变 $C_{TDS}:C_{Loss}$ 的值(简称为开销比),开销比大小在 1:10 和 1:160 以内变化,最终的实验结果如图 6 所示。

从图 6 可见,当开销比逐渐减小时,攻击损失增大,导致系统的服务率逐渐减小。当攻击损失增大时,AMTD 机制会相应地增加变换次数,来减缓系统服务率的降低。另外,可以清楚地看到,攻击密度较大的 trace2 和 trace1 相比而言,随着开销比的减小,系统服务率的降低速度更快,这说明攻击密度较大时,AMTD 的系统服务率的大小对开销比的变化更敏感。所以,给 C_{Loss} 加个权重因子,可以优化 AMTD 机制中 MTD 变换的触发条件,这样就能有效适应开销比发生变化的情况。

4.4 入侵检测提前量对服务率的影响

本实验关注的问题是,IDS 预警的提前时间(也就是 t_{Lead} 值,其均值为 ω)对采用 AMTD 机制的系统服务率的影响。参数设置除了 ω 值,其他值都和表 2 参数值一样。

本实验同 3.3 节实验一样,保持 MTD 变换开销为 20 s 不变,使 ω 值在 10 s 和 80 s 之间变化,以差值 5 s 递增,实验最终结果如图 7 所示。在实验过程中,若 $t_{lead} \geq C_{ADS}$,可认定 ADS 变换完成,否则认定 ADS 未完成。在图 7 中可发现,当 ω 值增大时,采用 AMTD 机制的系统服务率会不断增大,速度呈现先快后慢的趋势,即 ω 和

C_{ADS} 相近时,系统服务率增长速度较快,之后随着 ω 增大,系统服务率增长速度减缓。通过观察得到,当 $\omega \geq 1.5C_{ADS}$ 时,系统的服务率较高。所以,若要通过改善 IDS 系统预警来提高系统服务率,可把 $\omega \geq 1.5C_{ADS}$ 作为一个度量指标。另外,对攻击密度更大的 trace2 而言, t_{lead} 对采用 AMTD 机制的系统服务率的影响更大,所以,增大 IDS 预警的提前时间可快速提高系统服务率。

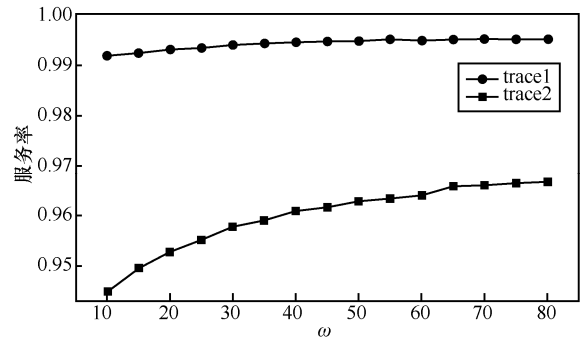


图7 ω 值对 AMTD 系统服务率的影响

5 结束语

本文首次提出了一个具有适应性的移动目标防御系统框架 AMTD,希望能有效实现系统在可用性—安全性—变换开销之间的均衡。AMTD 的适应性体现在 2 方面:一是防御方式的适应性,AMTD 中既可提供基于异常事件驱动的反应式防御(ADS 变换),又可提供基于计时器期满事件驱动的主动式防御(TDS 变换),并且通过科学的数学建模得出防御执行的触发条件;二是 MTD 变换间隔的适应性。每次 TDS 变换间隔的起始时刻是上一次 ADS/TDS 变换完成的时刻,且 TDS 变换所需的时长是采用本文之前建立的数学模型

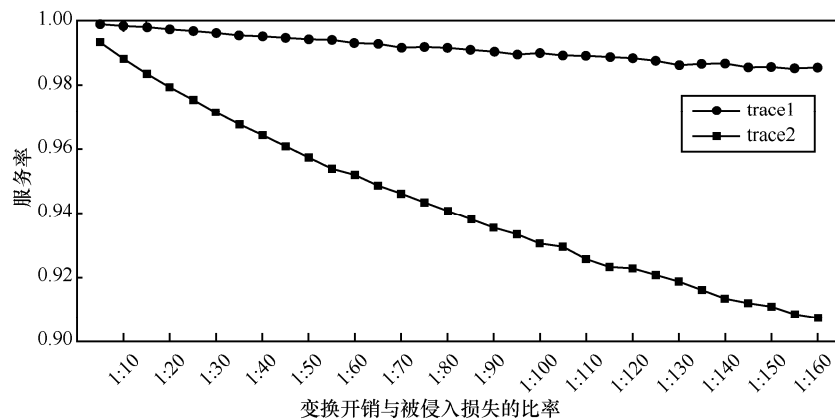


图6 变换开销与被侵入损失的比率对系统服务率的影响

和实际监测得来的参数值计算出来的, 所以变换时长具有一定的适应性。

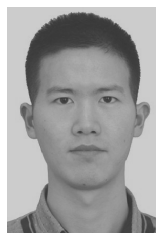
本文首先介绍了 AMTD 的系统组成和原理, 提出利用系统服务率来表示 MTD 变换的时间开销对系统可用性的影响, 并通过建立科学的数学模型来计算 AMTD 系统中 ADS 变换的触发条件和 TDS 变换的最优时间间隔。本文把每次 TDS 变换的起始时间设置为上一次 MTD 变换 (ADS/TDS) 的完成时刻 (避免在进行完 ADS 变换后又立刻进行 TDS 变换, 导致不必要的变换开销), 若发生系统被攻破的事件, 则设置为系统被攻破后恢复可用性的起始时间。

本文也详细描述了笔者设计的 AMTDsim 模拟器, 利用该模拟器进行了 4 个不同的实验, 来验证 AMTD 机制的有效性, 这 4 个实验分别是, 对采用 AMTD 机制和采用固定时间间隔变换机制的系统服务率进行比较、IDS 精度对采用 AMTD 机制的系统服务率的影响、单次变换开销与被攻击损失比的变化对系统服务率的影响、入侵检测警报的提前量对服务率的影响。最终的实验结果表明, 采用 AMTD 机制的系统要优于采用固定间隔的 MTD 机制的系统, 同时也说明, AMTD 机制的效果会受到 IDS 系统精度、入侵检测报警提前量、ADS/TDS 变换开销以及被攻击损失变化的影响。

参考文献:

- [1] LIU Y, PENG W, SU J. A study of IP prefix hijacking in cloud computing networks[J]. Security and Communication Networks, 2014, 7 (11): 2201-2210.
- [2] WANG T, WANG H, LIU B, et al. Further analyzing the sybil attack in mitigating peer-to-peer botnets[J]. KSII Transactions on Internet & Information Systems, 2012, 6 (10).
- [3] WANG F, WANG H, WANG X, et al. A new multistage approach to detect subtle DDoS attacks[J]. Mathematical and Computer Modeling, 2012, 55 (1): 198-213.
- [4] ZDNet C, ZACK W. PRISM: here's how the NSA wiretapped the Internet[EB/OL]. <http://www.zdnet.com/article/prism-heres-how-the-nsa-wiretapped-the-internet/>.
- [5] CODENOMICON. The heartbleed bug[EB/OL]. <http://heartbleed.com>.
- [6] CLARK A, SUN K, POOVENDRAN R. Effectiveness of IP address randomization in decoy-based moving target defense[C]//The 52nd IEEE Conference on Decision and Control. 2013: 678-685.
- [7] MANADHATA P. Game theoretic approaches to attack surface shifting[M]//Moving Target Defense II: Application of Game Theory and Adversarial Modeling. 2013: 1-13.
- [8] CROUSE M, PROSSER B, FULP E. Probabilistic performance analysis of moving target and deception reconnaissance defenses[C]//The Second ACM Workshop on Moving Target Defense. 2015: 21-29.
- [9] ZHU Q, BAŞAR T. Game-theoretic approach to feedback-driven multi-stage moving target defense[C]//The 4th International Conference on Decision and Game Theory for Security-Volume 8252.
- [10] 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.
- [11] NITRDSubcommittee. National cyber leap year summit 2009 co-chairs' report[EB/OL]. https://www.nitrd.gov/nitrdgroups/index.php?title=Category:National_Cyber_Leap_Year_Summit_2009.
- [12] AZAB M, HASSAN R, ELTOWEISSY M. ChameleonSoft: a moving target defense system[C]//The 7th International Conference on Collaborative Computing: Networking, Applications and Worksharing (CollaborateCom). 2011: 241-250.
- [13] OKHRAVI H, COMELLA A, ROBINSON E, et al. Creating a cyber moving target for critical infrastructure applications[M]//Critical Infrastructure Protection V. Berlin Heidelberg: Springer, 2011: 107-123.
- [14] HUANG Y, GHOSH A. Introducing diversity and uncertainty to create moving attack surfaces for Web services[M]//Moving Target Defense: Creating Asymmetric Uncertainty for Cyber Threats. 2011: 131-151.
- [15] DEBROY S, CALYAM P, NGUYEN M, et al. Frequency-minimal moving target defense using software-defined networking[C]//2016 International Conference on Computing, Networking and Communications (ICNC). 2016: 1-6.
- [16] LUO Y, WANG B, WANG X, et al. RPAH: random port and address hopping for thwarting internal and external adversaries[C]//2015 IEEE Trustcom/BigDataSE/ISPA. 2015: 263-270.
- [17] 周志华. 机器学习[M]. 北京: 清华大学出版社, 2016.
- [18] BERAUD P, CRUZ A, HASSELL S, et al. Using cyber maneuver to improve network resiliency[C]//2011 Military Communications Conference (MILCOM 2011). 2011: 1121-1126.
- [19] KUHL M E, KISTNER J, COSTANTINI K, et al. Cyber attack modeling and simulation for network security analysis[C]//The 39th Conference on Winter Simulation. 2007: 1180-1188.
- [20] BERAUD P, CRUZ A, HASSELL S, et al. Cyber defense network maneuver commander[C]//2010 IEEE International Carnahan Conference on Security Technology (ICCST). 2010: 112-120.

作者简介:



刘丹军 (1994-), 男, 湖北潜江人, 国防科技大学硕士生, 主要研究方向为网络安全、二进制安全。

蔡桂林 (1982-), 女, 湖北浠水人, 博士, 主要研究方向为网络安全、移动目标防御。

王宝生 (1970-), 男, 河北黄骅人, 博士, 国防科技大学研究员, 主要研究方向为网络与信息安全。