

动态平台技术防御攻击的瞬态效能量化分析

蔡雨彤, 常晓林, 石 禹, 陈 志

智能交通数据安全与隐私保护技术北京市重点实验室, 北京交通大学计算机与信息技术学院 北京 中国 100044

摘要 移动目标防御(Moving Target Defense, MTD)是一种主动防御策略, 而动态平台技术(Dynamic Platform Techniques, DPT)是 MTD 在平台层面的一种具体实现方案, 其通过在脆弱网络系统中构建随机动态变化的运行平台, 来提高脆弱网络系统中网络服务被探测和被攻击的复杂度, 从而提高关键网络服务的安全性。目前状态空间模型已应用于 MTD 效能的量化分析, 但仅用于稳态分析; 而对于关键网络服务, DPT 瞬态效能量化分析极为重要。本文通过分析脆弱网络系统中网络服务的可生存性, 来实现 DPT 防御攻击的瞬态效能量化分析。本文构建了基于马尔可夫链的可生存性模型, 用于捕捉从系统漏洞被披露到漏洞被消除这段时期内, 攻击者、网络服务和防御机制三者之间的动态行为; 定义了相关评估指标并给出了计算公式; 进行了数值实验, 利用构建的模型和指标计算公式, 分析关键参数对 DPT 效能的影响, 并设计了被动防御机制作为对比实验, 以突显 DPT 的效能。

关键词 移动目标防御; 动态平台; 瞬态效能; 马尔可夫链; 可生存性; 主动防御

中图法分类号 TP309 DOI号 10.19363/J.cnki.cn10-1380/tn.2019.07.04

Analyzing Transient Effectiveness of Dynamic Platform Technique in Resisting Attacks

CAI Yutong, CHANG Xiaolin, SHI Yu, CHEN Zhi

Beijing Key Laboratory of Security and Privacy in Intelligent Transportation, School of Computer and Information Technology,
Beijing Jiaotong University, Beijing 100044, China

Abstract Moving target defense (MTD) is a proactive defense strategy. Dynamic Platform Technique (DPT) is a specific implementation of MTD strategy at the platform level. It increases the complexity of exploring and attacking network services by constructing a randomly and dynamically changing execution platform in vulnerable network systems, thus the security of critical network service is improved. State-space models have been applied to the quantitative analysis of MTD effectiveness, but only for steady-state analysis. For critical network services, quantitative analysis of DPT transient effectiveness is more important. This paper aims to quantitatively analyze DPT effectiveness in resisting attacks by quantitatively analyzing the DPT effectiveness in improving network service survivability. The paper constructs a survivability model based on Markov chain to capture the dynamic behavior between attackers, network services and defense mechanism during the period from system vulnerabilities being disclosed to vulnerabilities being eliminated. The relevant metrics are defined and the formulas for calculating metrics are given. Numerical experiments are finally constructed to assess the impact of key parameters on DPT effectiveness by using the model and calculation formulas. A reactive defense mechanism is designed as comparison experiments to show the effectiveness of DPT.

Key words moving target defense; dynamic platform; transient effectiveness; markov chain; survivability; proactive defense

1 引言

软件漏洞是一个系统中可以被利用来发动攻击的弱点, Symantec 公司 2018 年发布的互联网安全威胁报告^[1]中显示, 2017 年被披露的漏洞数量是 8718 个, 相比 2016 年的数据增长了 13%。随着企业网络系统越来越庞大复杂, 2018 年将有更多的漏洞被披

露出来^[2]。

攻击者发起攻击通常会经历以下四个阶段: (1)通过已披露的漏洞获得访问目标系统的权限; (2)尝试各种方法驻扎在系统中; (3)搜索关键数据, 为进一步窃取或修改数据做准备; (4)通过改变未经授权的数据和/或泄露敏感数据, 来破坏系统安全性。攻击面是指可能被攻击者用于攻击的漏洞的集合。移动目

通讯作者: 常晓林, 博士, 教授, Email: xlchang@bjtu.edu.cn。

本课题得到国家自然科学基金(No.61572066 和 No.U183610024)资助。

收稿日期: 2018-09-30; 修改日期: 2018-12-24; 定稿日期: 2019-01-08

标防御(Moving Target Defense, MTD)作为一种主动的防御策略,通过不断改变攻击面,使攻击者很难到达最后一个攻击阶段,降低了系统被成功攻击的概率,从而提高系统安全性。因此,在分析 MTD 提高网络服务可生存性的瞬态效能时,有必要考虑攻击过程的细节。

动态平台技术(Dynamic Platform Techniques, DPT)是 MTD 在平台层面的一种具体实现方案,可以有效地防御针对网络系统中关键服务的攻击。DPT 通过构建随机动态变化或多态虚拟的系统运行平台,动态地改变平台属性,实现平台攻击面的变化,从而增加攻击者的成本,提高平台上运行的服务的可生存性。图 1 形象地说明了攻击者攻击目标系统时,网络系统中的关键服务正在平台之间迁移,使得针对关键网络服务的攻击变得困难。

提高关键网络服务在恶意攻击下的可生存性尤其重要,这已经得到了服务提供商的共识。DPT 可以有效地提高服务的可生存性,而对 DPT 瞬态效能的量化分析可以帮助提高系统关键服务的供应水平。本文将网络服务的可生存性定义为抵御与漏洞相关的恶意攻击并实现预先声明的服务质量的能力的一种瞬态指标。本文主要研究了动态平台技术对提高网络系统中关键服务可生存性的瞬态效能。另外,本文假设,在漏洞被披露后,服务提供商将设计一种被动防御机制以消除漏洞,此设计过程称为修复过程。在修复过程中,基于动态平台技术的 MTD 策略将被启用,以减少攻击造成的损害^[3]。

目前,基于模型的定量分析技术已经被提出并用于研究 MTD 技术的效能,可以分为两类:基于非状态空间模型的建模技术和基于状态空间模型的建模技术。非状态空间模型技术不需要状态信息,即不用产生底层的状态空间,此外,该技术不能捕捉到时间依赖关系^[4],因此具有较低的建模能力。而现有的评估 MTD 效能的状态空间模型只关注于稳态下的表现,并未做出对瞬态效能的量化分析。

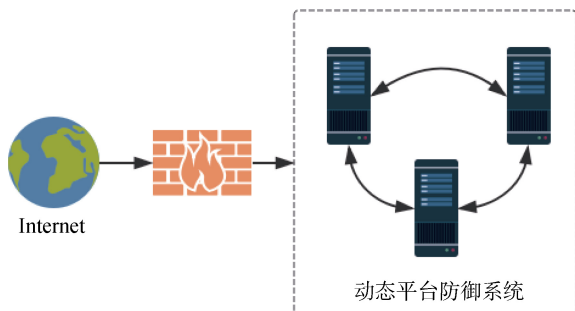


图 1 基于动态平台技术的网络系统
Figure 1 DPT-based network system

本文提出了一个可生存性分析模型,描述了从系统漏洞被披露到漏洞被消除这段时期内,攻击者、网络服务和防御机制三者之间的动态状态。对公开文献的调研显示,这是首次使用状态空间模型对动态平台技术抵御攻击的瞬态效能进行量化分析,本文的主要贡献概括如下:

- 提出了一个基于马尔可夫链的分析模型,分析动态平台技术提高网络系统中关键服务可生存性的瞬态效能,并使用随机奖励网(Stochastic Reward Net, SRN)来生成和求解所提出的马尔可夫模型。
- 定义了一系列与可生存性相关的指标,包括瞬态指标和累积指标,以度量网络服务可生存性,并给出了计算公式。
- 进行数值分析以研究动态平台技术在提高网络关键服务可生存性方面的效能。数值结果为设计有效的动态平台防御机制提供了指导。

与文献[5]中相同,本文所有时间间隔都被假设为是相互独立且服从指数分布的,因此模型符合齐次连续时间马尔可夫链(CTMC)的特征。有许多技术可以放宽这个假设^[6],我们将此部分作为未来工作。本文的其余部分安排如下。第 2 节介绍了相关工作和 SRN 预备知识。第 3 节介绍了系统描述,SRN 模型和指标定义。第 4 节介绍了数值分析和讨论。第 5 节介绍了结论和未来的工作。

2 相关工作与预备知识

本章首先对移动目标防御的相关工作进行了介绍,然后介绍了本文涉及的有关 Petri 网的预备知识。

2.1 移动目标防御技术研究

目前,MTD 现有研究成果根据研究内容可以分为两大类:MTD 机制设计和 MTD 安全效能评估,而现有的基于模型的 MTD 效能量化分析成果可分为以下两类:基于非状态空间模型的建模技术,如攻击图(AttackGraph, AG)^[7-11];基于状态空间模型的建模技术,如马尔可夫模型^[5,12-15]。

Hong 等人^[7]将 MTD 技术分为扰乱(shuffle)技术、多样性(diversity)技术和冗余(redundancy)技术三类,并通过一个两层图模型来进一步评估其效能,但是,文献[7]中没有提出具体的安全性分析。Ge 等人^[8]开发了两种主动防御机制和重置(reconfiguration)算法来重置基于软件定义网络的物联网(SD-IoT)拓扑结构,并使用基于 AG 的模型分析了 SD-IoT 网络的性能和安全性。Okhravi 等人^[9]使用 AG 对应用程序所面临的威胁进行分级,然后针对不同的威胁等

级设计不同的迁移方案。Wang 等人^[10]提出了一种类似于 AG 的建模方法, 将网络多样性建模为一种安全指标, 用于评估网络对潜在零日攻击的鲁棒性。Almohri 等人^[11]提出了一种概率图模型和算法, 用于分析复杂网络的安全性, 从而进一步降低攻击成功的概率。然而, 这些基于非状态空间模型的量化分析无法对攻击行为和防御机制之间的动态状态进行细粒度的分析, 因为其没有状态信息, 也不允许时间依赖性。

Okhravi 等人^[12]提出了一个模型, 通过离散时间马尔可夫链(DTMC)来量化分析动态平台技术的效能。Hu 等人^[13]构建了一个基于自适应网络防御(Adaptive Cyber Defense)的部分可观测马尔可夫决策过程(POMDP)问题, 并提出了在线算法对其求解。Connell 等人^[14]使用基于 CTMC 的模型对不同资源重置率下 MTD 机制的可用性和性能进行定量分析。Maleki 等人^[15]提出了基于马尔可夫模型的 MTD 分析框架, 并定义了安全能力(security capacity), 以评估 MTD 策略的效能。Anderson 等人^[15]分别基于闭合解和随机 Petri 网(Stochastic Petri Net, SPN)提出了两种分析模型, 以分析 MTD 对降低成功攻击概率的效能。与本文提出的状态空间模型不同, 这些模型旨在对 MTD 稳态效能进行量化分析。表 1 显示了本文的研究在 MTD 效能评估上与现有状态空间建模工作之间的比较。

表 1 与现有基于状态空间的模型分析作对比

Table 1 Comparison of analysis based on state space models

方法 模型	瞬态	稳态	多阶段攻击模型
Okhravi 等人 ^[12]	-	√	-
Hu 等人 ^[13]	-	√	√
Connell 等人 ^[14]	-	√	-
Maleki 等人 ^[14]	-	√	-
Anderson 等人 ^[15]	-	-	√
本文	√	√	√

可生存性是一种瞬态指标, 用于描述系统在发生意外事件后及时恢复预先定义的服务的能力^[6]。当系统的某个部分发生损坏或整个系统受损时, 其量化分析有助于提高系统关键服务的供应水平。最近, Chang 等人^[16]对系统安全生存性进行了定量评估。与文献[16]不同, 本文研究了同时部署主动和被动防御策略以减少或消除恶意软件造成的安全损害的情况。

除建模技术外, 仿真(simulation)也被用来评估

MTD 的效能。Zaffarano 等人^[17]提出了一个定量分析框架, 并使用仿真实验得到大量数据, 进而评估 MTD 策略的效能。Zhuang 等人^[18]提出了企业网络中 MTD 的初步设计方案, 他们通过主动改变基于仿真的网络参数, 研究敌手的成功机会。基于仿真的 MTD 效能评估的一个问题是这些技术是依赖于具体案例的, 即它们仅反映了引述的特定示例, 本文基于模型的 MTD 分析是对这些基于仿真的工作的补充。

最近, 各种 MTD 机制已经被提出并应用到各个方面, 例如软件应用、新型网络技术和执行环境。Jafarian 等人^[19]使用基于虚拟 DNS 条目和软件定义网络(Software Defined Network, SDN)的 IP 虚拟化方案来对敌手隐藏网络资产, 每个主机通过使用 OpenFlow 都与一系列虚拟 IP 地址相关联, 并在其 IP 池中实现 IP 地址突变。Amirreza 等人^[20]提出了一个名为 WebMTD 的 MTD 机制, 可以阻碍 Web 代码注入攻击。Richard 等人^[21]提出了一种名为 PHEAR (Packet Header Randomization)的移动目标防御技术, 它建立在现有的 SDN 协议和标准之上, 通过从网络流量中删除隐式和显式标识符来保护企业/园区网络中的流量。类似地, U-TRI(Unlinkability-Through Random Identifier)通过使用结构化随机虚拟标识符来实现 SDN 上的不可链接性^[22]。Carter 等人^[23]使用博弈论来决定在给定的可用动态平台中迁移的更佳选择。Hong 等人^[24]说明了随机分配问题, 并开发了一种启发式算法来重新配置网络, 并给出近似最优解。Lei 等人^[25]提出了一种基于博弈论的机制来解决 MTD 中的最优策略问题。基于模型的 MTD 效能的定量分析在 MTD 机制的设计中起着关键作用, 这些模型可以解释这些机制效能背后的原因。

2.2 Petri 网相关概念介绍

本节介绍随机 Petri 网(SPN)的一些基本知识。PetriNet(PN)形式及其理论首先由 C.A.Petri 于 1962 年描述^[26]。PN 是一种二部图, 其节点可被划分为两个集合, 称为库索(place)和变迁(transition)。图中的定向弧将 places 连接到 transitions, 称为输入弧; 以及将 transitions 连接到 places, 称为输出弧。PN 的标识(marking)是列出 PN 所有 place 中的 token 数量的向量。通过将令牌(token)与 place 相关联就得到 MarkedPetriNet, 一个 MarkedPetriNet 就是一个五元组 (P, T, I, O, M) ^[27], 其中:

$P = \{p_1, p_2, \dots, p_n\}$ 是 n 个 place 的集合, 在图中绘制为圆圈;

$T = \{t_1, t_2, \dots, t_n\}$ 是 n 个 transition 的集合, 在图中

绘制为条形(immediate transition)或矩形(timed transition);

I 是 transition 的输入关系, 在图中通过从 place 指向 transition 的有向弧表示;

O 是 transition 的输出关系, 在图中通过从 transition 指向 place 的有向弧表示;

$M = \{m_0, m_1, m_2, \dots, m_i, \dots\}$ 是 marking 随时间推移而变化的序列, 其中 m_0 是初始标识。

随机 Petri 网是通过引入随机的触发时间(firingtimes)与 transition 相关联而对 PN 的扩展。在 SPN 的基础上, SRN 还引入了卫式函数(guardfunctions), 一般标记依赖性(general marking dependency), 可变基数弧(variable cardinality arcs)和奖励结构的叠加^[28]。本节只介绍一下 guard functions。一个 guard function $g(\cdot)$ 是一个布尔函数, 且与 transition 相关联, 仅当 transition 满足标识 M 中的所有输入和限制条件时, 即当 $g(M) = TRUE$ 时, guardfunction 被允许且 transition 触发。Guardfunction 在表达复杂的相互依赖性和简化模型结构时非常实用, 此外, guardfunction 在实现状态截断时也很有用。

表 2 变量定义
Table 2 Variable definition

变量	定义	期望
$1/\alpha$	攻击者获取对目标平台的访问权限的平均时间	25hours
$1/\beta$	恶意代码完全驻扎在平台上的平均时间	15min
$1/\gamma$	数据从平台中被泄露的平均时间	30min
$1/\delta$	恶意代码在平台中搜索数据的平均时间	15min
$1/\lambda$	服务在一个平台上运行的平均时间	1hour
$1/\theta$	被动防御机制生效的平均时间	30days

3 分析模型

本节首先对要研究的系统进行介绍, 该系统的 SRN 模型见第 3.3 节。然后给出定量指标定义和计算公式, 下文所使用的变量的定义如表 2 所示。

3.1 系统描述

在一个部署了动态平台技术的网络系统中, 服务提供商预备了多个平台来运行关键服务, 但在某一时刻只有一个平台用于服务执行, 服务提供商每隔一段时间在平台之间切换关键服务, 因此攻击者无法确定服务正在运行在哪个平台上。在不失一般性的情况下, 本文假设与漏洞相关的恶意软件已准备就绪, 攻击者会在漏洞披露之后立刻开始攻击, 同时系统开始设计消除漏洞的被动防御机制, 只要系统被动防御机制准备就绪, 则所有平台立即部署,

此后也就不存在与此漏洞相关的进一步成功攻击。这些假设只是为了方便后面描述。

在被动防御机制生效之前, 攻击者会持续发起攻击, 同一时刻只有一个平台会受到攻击, 平台每运行一段时间后, 服务将被随机地迁移至另一个平台, 此时无论攻击者是否攻击成功, 都将被迫停止攻击当前平台, 服务迁移后, 平台上不会留下任何恶意软件。当攻击者在平台中发现有价值的数据并对其进行攻击时(例如通过 Internet 向远程位置发送数据), 我们就认为此次攻击是成功的。在本文的模型中, 规定一次成功的攻击需要经历以下四个阶段:

- 开发(exploit): 攻击者通过各种手段利用所披露的漏洞获取对目标系统的访问权限。
- 感染(infect): 攻击者尝试各种方法侵入平台并使恶意软件在选定的平台上驻扎。
- 搜索(search): 攻击者定期在受感染平台中查找关键数据。
- 泄露(exfiltrate): 攻击者通过 Internet 将数据发送到远程位置。

一旦发生服务迁移, 攻击者就必须回到初始阶段(exploit), 即攻击者在之前平台上的努力是徒劳的。我们假设攻击者每次发起攻击都是从 N 个平台中随机选择一个平台, 每台被选取的概率相同, 这意味着同一个平台可能被连续多次选取。服务提供商从剩下的 $N-1$ 个平台中等可能地选择平台以进行服务迁移。本文假设所有时间间隔都是指数分布的。

下面通过 $N=2$ 来举例说明系统状态转换。定义三元组 (i, j, k) 来表示每个系统状态的特征, 其中, i 代表攻击者选择的平台, j 代表服务运行的平台, k 代表攻击者的当前状态。表 3 总结了 (i, j, k) 的全部情况。例如, 状态 $(1, 1, 0)$ 表示攻击者选择平台 1, 而服务也在平台 1 上运行, 并且攻击者正在入侵平台 1。请注意, 某些元组值没有意义, 例如 $(0, 1, 1)$ 和 $(0, 1, 2)$ 。

表 3 三元组中元素的取值
Table 3 Settings of elements in the tuple

	0	1	2
i	没有选择平台	选择平台 1	选择平台 2
j	-	服务运行在平台 1	服务运行在平台 2
k	exploit / infect	search	exfiltrate

图 2 给出了状态转换图。当漏洞披露时, 服务正在平台 1 或平台 2 上执行。当攻击者以 $1/N$ 的概率选择某一平台时, 系统以 $\alpha/2$ 的速率由 $(0, j, 0)$ 转移到 $(1, j, 0)$ 状态或 $(2, j, 0)$ 状态。此解释也适用于速率 $\delta/2$ 。无论攻击者选择哪个平台, 攻击者都会先进入

exploit 阶段, 但只有当 $i=j$ 时, 攻击才会成功。此外, 在攻击者 *exploit* 成功后, 恶意代码将开始注入平台。一旦成功部署恶意代码, 也就是 $k=1$, 即 *infect* 阶段结束, 攻击者将开始搜索基本信息, 然后窃取感兴趣的数据。*search* 状态和 *exfiltrate* 状态, 即(1,1,1)和(1,1,2), (2,2,1)和(2,2,2), 将以速率 δ 和速率 γ 交替进行, 直到服务迁移到另一个平台。状态(1,2,1)和(2,1,1)无法进入 *search* 和 *exfiltrate* 阶段, 因为服务不在此平台中。 θ 表示被动防御机制生效的速率。

攻击者旨在窃取尽可能多的数据, 而服务提供商旨在最大限度地降低数据泄露的风险, 因此, 可以使用攻击和服务不在同一平台中共存的概率来评估该系统中网络服务的生存性。此外, 还考虑了成功攻击的瞬时和累积指标, 全部指标定义如表 4 所示。

表 4 指标定义

Table 4 Metric definition

指标	定义
m_1	在时刻 t 的平均成功攻击次数
m_2	在 $[0, t]$ 时间段内平均累积成功攻击次数
m_3	在 $[0, t]$ 时间段内攻击者处于攻击成功状态的累积时长
m_4	在时刻 t , 服务处于安全的概率(即服务和攻击者处在不同平台上)
m_5	在时刻 t 的平均攻击收益
m_6	在 $[0, t]$ 时间段内平均累积攻击收益

瞬态指标是某一时刻的测量值, 相应地, 累积指标是某一时间段内的测量值。因此, m_1 , m_4 和 m_5 是瞬态指标, 表示在多阶段攻击下在时刻 t 的系统属性。指标 m_2 , m_3 和 m_6 是区间 $[0, t]$ 中的累积指标。

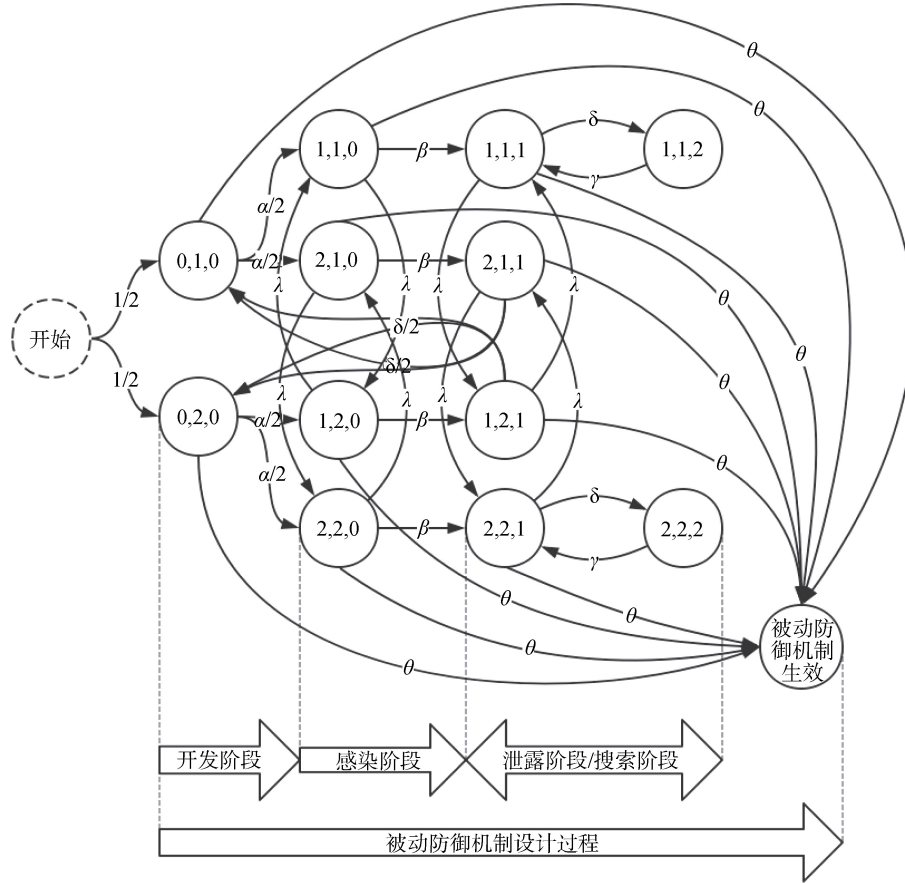


图 2 系统状态转移图

Figure 2 System state transition diagram

3.2 SRN 模型

如图 2 所示, 即使在 $N=2$ 的情况下, 状态转换关系也非常复杂。随着 N 的增加, 系统将会有更多的状态, 而且状态交互也会更复杂。当 N 很大时, 很难手工推导出连续时间马尔可夫链无穷小生成元, 因此需要建立 SRN 模型。借助软件工具 SPNP^[29], 可以

将模型和参数作为输入然后自动地得出结果, 我们可以先使用 SPNP 来建立 N 较小时的 SRN 模型和计算指标的公式, 然后通过导出 N 较小时的 SRN 模型的源代码, 观察其特征, 再用 Python 编写程序来生成任意 N 的 SRN 模型和指标计算公式。在本文中, 由于页面限制, 我们省略了基于 Python 的代码。本节

的其余部分首先介绍 $N=3$ 的 SRN 模型, 然后给出指标的计算公式。

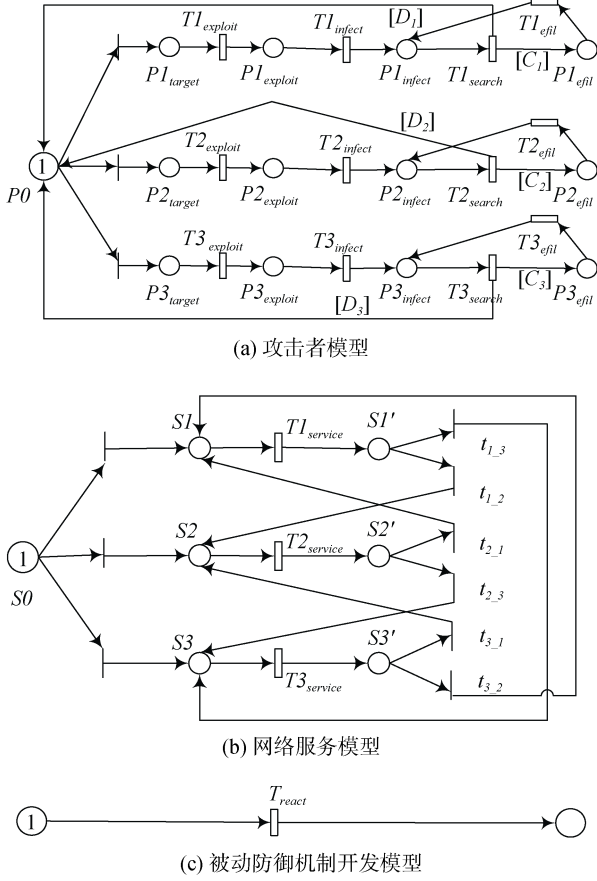


图 3 SRN 模型

Figure 3 SRN models

图 3 显示了部署了动态平台技术的系统中网络服务可生存性分析的 SRN 模型, 其中系统模型中有 3 个平台。Guardfunctions 的定义在表 5 中给出。关键服务在 3 个平台之一上执行。在图 3(b)中, 当 $Ti_{service}$ 触发时, 一个 token 将从 Si 转移到 Si' 中, 表示该服务周期完成。当有 token 处在 Si' 中时, $t_{i,j} (i \neq j)$ 将会触发, 一个 token 将从 Si' 转移到 Sj 中, 代表服务从平台 i 迁移到平台 j 上。这里, $i, j=1,2,3$ 仅表示平台序号。当发起新的攻击时, 3 个 immediate transitions 中的 1 个触发, 表示选择了 N 个平台中的 1 个。然后, 从 $P0$ 中取出一个 token, 并将一个 token 存放在 $P1_{target}$ 、 $P2_{target}$ 或 $P3_{target}$ 中。 $Pi_{exploit}$, Pi_{infect} 和 Pi_{efil} 分别代表攻击者在平台 i 上处于某一相应的攻击阶段。当 $Ti_{exploit}$ 触发时, 将从 Pi_{target} 取出一个 token, 并将一个 token 放入 $Pi_{exploit}$, 表示恶意代码(如木马或蠕虫)已成功驻扎在平台上。当 Ti_{infect} 触发时, 将从 $Pi_{exploit}$ 取出一个 token, 并将一个 token 放入 Pi_{infect} , 表示已在平台上部署恶意代码。当 Ti_{search} 触发时, 将从

Pi_{infect} 中取出一个 token, 并将一个 token 放入 Pi_{efil} 或 $P0$ 中, 具体选择取决于 guardfunction C_x 或 D_x 。当攻击经历完 *search* 阶段后将进行判断, 若 $C_x=TRUE$, 则可进入 *exfiltrate* 阶段, 从而 Ti_{efil} 触发。值得说明的时, 一旦 Ti_{efil} 触发, 则不需再关注服务是否迁移到另一个平台, 因为一旦恶意代码成功搜索关键数据, 它就会开始复制并发送到远程位置来窃取数据, 即便服务已经迁移到其他平台上, Ti_{efil} 仍然会触发。最后, 在图 3(c)中, 当 T_{react} 触发时, 被动防御机制生效。

表 5 卫式函数定义

Table 5 Guard function definition

名称	定义
$[C_x], x \in (1,2,3)$	if $\#S_x = 1$, then return 1, else return 0
$[D_x], x \in (1,2,3)$	if $\#S_x = 1$, then return 0, else return 1

在 3.1 节中定义的 6 个指标的计算公式给出如下:

- m_1 : $\sum_i Ti_{efil}$ 在时刻 t 的吞吐量;
- m_2 : $\sum_i Ti_{efil}$ 在 $[0, t]$ 时间段内的累积吞吐量的期望;
- m_3 : $t \sum_i Pi_{efil}$ 在 $[0, t]$ 时间段内的累积 token 数量的期望;
- m_4 : $(1 - \sum_i Pi_{efil})$ 在时刻 t 的 token 数量的期望;
- m_5 : $\omega_i Ti_{efil}$ 在时间 t 的吞吐量, 其中奖励率 ω_i 是平台 i 的平均奖励;
- m_6 : $\omega_i \sum_i Ti_{efil}$ 在 $[0, t]$ 时间段内的累积吞吐量的期望。

4 数值分析与讨论

本节将使用 SPNP 软件包^[29]进行数值分析来评估本文所设计的 SRN 模型, 变量缺省值如表 2 所示。注意, θ 的值根据文献[30]设置, 其他参数的值设置得相对较小, 以使动态平台技术的防御作用更明显。我们对以下两种场景进行了比较分析, 以突出部署了动态平台技术的网络系统的效能:

场景 1: 部署了动态平台技术和被动防御机制的脆弱网络系统。

场景 2: 仅部署了被动防御机制的脆弱网络系统, 其中, 服务仅在 N 个平台中的一个平台上运行且从不迁移。

根据上一节中定义的指标, 我们将数值结果分为两类: 累积结果(图 4 和图 6)和瞬态结果(图 5 和图 7)。图 4 的(a)和(b)分别显示了场景 1 和场景 2 在平台数量从 3 到 8 的平均累积时长。从图 4 中可以观察到:

- 在场景 1 中, N 无论取何值, 其平均累积时长(m_3)都是在大约 1 小时后线性增加。主要因为 m_3 中的 $\sum_i P_{i_{efl}}$ 在一定时间后接近常数。本文假设设计和部署被动防御机制的时间很长(参见表 2, 假设为 30 days), 以突出动态平台技术的效能。当这种被动防御机制准备就绪时, 无论 N 取哪个值, m_3 的值都不会改变。
- 在场景 2 中, N 无论取何值, 其平均累积时长(m_3)都随着时间 t 的增加而线性增加。主要因为一旦攻击者入侵“正确的”平台, 就再也不需要离开, 所以 m_3 的值就会稳步增长。图 4(b)还显示了前 20 hours 的详细结果, 以便与图 4(a)中的结果进行比较。
- 随着 N 的增加, 平均累积时长(m_3)随时间增加得更快。对于特定的时刻 t , 在 $N = N_1$ 时的平均持续时间约等于 $N = N_2$ 时的平均持续时间的 $\frac{N_1}{N_2}$ 倍。主要因为对于每个 $i \in N$, $P_{i_{efl}}$ 近似于常数。
- 在任何特定时刻 t , 场景 1 中 m_3 的值远小于场景 2 中的 m_3 的值, 这意味着动态平台技术显著提高了服务可生存性。

图 5 和图 6 分别显示了场景 1 中 N 取不同值时成功攻击次数的瞬态值(m_1)和累积值(m_2)。从图 5 可观察到成功攻击次数先增加然后趋于稳定。因为当服务刚开始在平台上运行时, 攻击者需要一定时间才能进行感染。图 6 表明 N 的取值不同时, 成功攻击的累积数量与图 4 具有相似的趋势。

图 7 显示了在平台数不同时场景 1 比场景 2 具有更高的安全概率(m_4)。在场景 1 和场景 2 中, 由于没有攻击, 在初始时刻概率等于 1, 几个小时后, 服务安全的概率在场景 1 中变得稳定。可以观察到, 平台的数量 N 也会影响预期结果。在场景 2 中, 稳定概率是一个非常低的值, 这也意味着动态平台技术显著提高了服务的可生存性。 N 无论取何值, 系统在时刻 t 处安全的概率最终趋近于相同的值, 因为在场景 2 中, 指标 m_4 实际上接近于 $\frac{\lambda}{\lambda + \delta}$ 。

5 结论与未来工作

动态平台技术具有多样化、多实例、随机化的

特性, 可以尽可能地阻碍网络攻击对服务的损害, 大大提高网络服务的可生存性。本文展示了一个可生存性分析模型, 对动态平台技术抵御攻击的瞬态效能进行了量化分析。使用随机奖励网生成马尔可夫模型并获得模型解, 定义了多种可生存性指标, 其产生的数值结果用于研究关键参数对网络服务可生存性的影响。

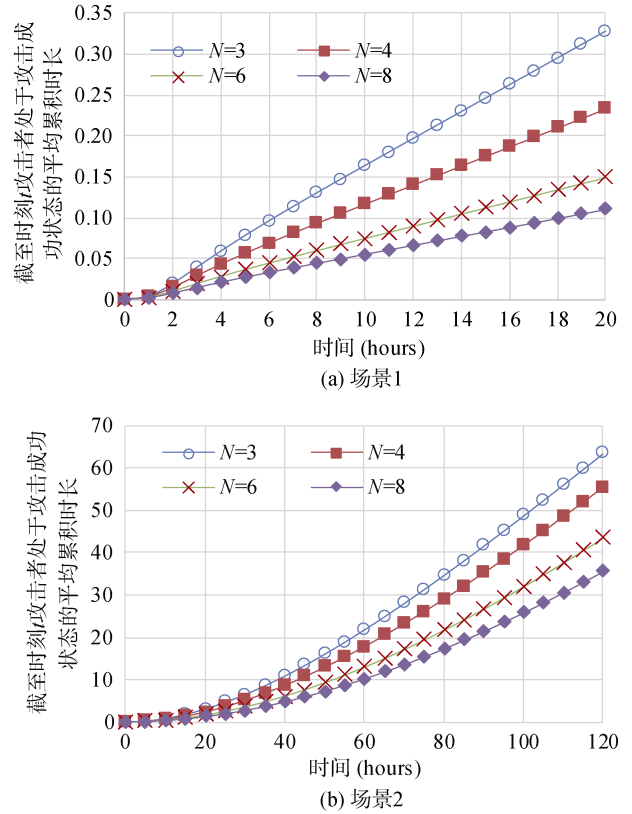


图 4 不同 N 截至时刻 t 攻击者处于攻击成功状态的平均累积时长(m_3)

Figure 4 Mean accumulated duration that the attacker stays in the successful attack state by time t under different N (metric m_3)

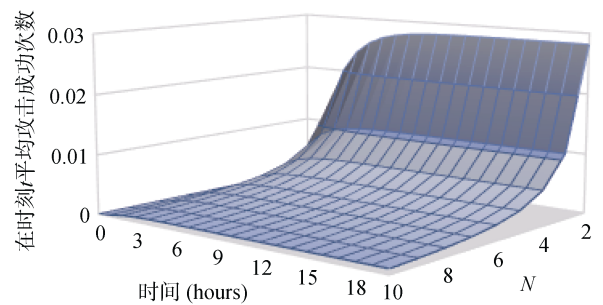


图 5 不同 N 在时刻 t 平均攻击成功次数(m_1)
Figure 5 Mean number of successful attacks at time t under different N (metric m_1)

本文假设攻击策略: 在发起新攻击时从 N 个平台中选择一个平台。但攻击者可能会攻击与上一个

受攻击平台相同的平台, 所以下一项研究将比较在不同攻击策略下动态平台技术的瞬态效能。

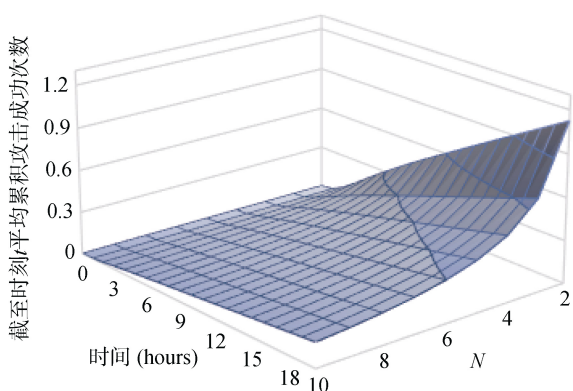
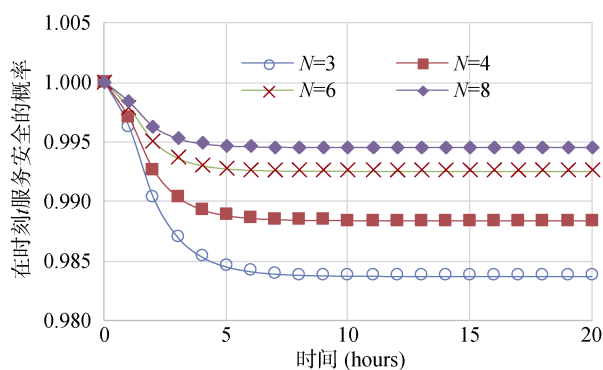
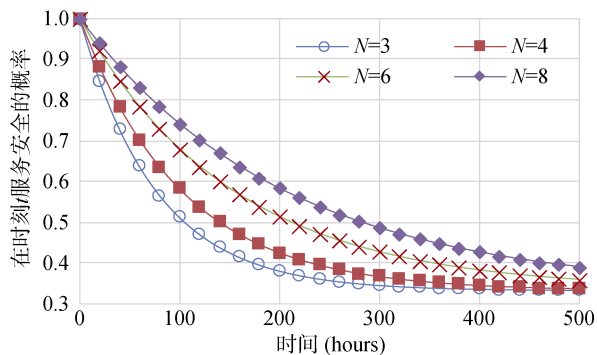


图 6 不同 N 截至时刻 t 平均累积攻击成功次数(m_2)

Figure 6 Mean accumulated number of successful attacks by time t under different N (metric m_2)



(a) 场景1



(b) 场景2

图 7 不同 N 在时刻 t 服务安全的概率(m_4)

Figure 7 Probability that the system is secure at time t under different N (metric m_4)

参考文献

- [1] "Symantec 2018 Internet Security Threat Report," Symantec, <https://www.symantec.com/security-center/threat-report>, Apr. 2018.
- [2] "Trend Micro Predicts 2018 Cyberattacks Will Rely on Vulnerabilities," Trend Micro, <http://newsroom.trendmicro.com/press-release/cyberthreat/trend-micro-predicts-2018-cyberattacks->

will- rely-vulnerabilities, Jan. 2018.

- [3] H. Okhravi, E. I. Robinson, S. Yannalfo, P. W. Michaleas, J. Haines, A. Comella, "TALENT: Dynamic Platform Heterogeneity for Cyber Survivability of Mission Critical Applications," in Conf. Secure and Resilient Cyber Architecture (SRCA'10), 2010.
- [4] K. Trivedi and A. Bobbio, "Reliability and Availability Engineering: Modeling, Analysis, and Applications," Cambridge University Press, 2017.
- [5] H. Maleki, S. Valizadeh, W. Koch, A. Bestavros, M. V. Dijk, "Markov Modeling of Moving Target Defense Games," in MTD@CCS, pp. 81-92, 2016.
- [6] X. Chang, J. M. Martinez, K. S. Trivedi, "Transient performance analysis of smart grid with dynamic power distribution," *Information Sciences*, vol. 422, pp. 98-109, 2018.
- [7] J. B. Hong, D. S. Kim, "Assessing the Effectiveness of Moving Target Defenses Using Security Models," *IEEE Trans. Dependable and Secure Computing*, vol. 13, no. 2, pp.163-177, 2016.
- [8] M. Ge, J. B. Hong, S. E. Yusuf, D. S. Kim, "Proactive defense mechanisms for the software-defined Internet of Things with non-patchable vulnerabilities," *Future Generation Computer Systems*, vol. 78, pp. 568-582, 2018.
- [9] H. Okhravi, A. Comella, E. Robinson, J. Haines, "Creating a Cyber Moving Target for Critical Infrastructure Applications Using Platform Diversity," *International Journal of Critical Infrastructure Protection*, vol.5, no. 1, pp. 30-39, 2012.
- [10] L. Wang, M. Zhang, S. Jajodia, A. Singhal, M. Albanese, "Modeling Network Diversity for Evaluating the Robustness of Networks against Zero-Day Attacks," *Lecture Notes in Computer Science*, vol. 8713, pp. 494-511, 2014.
- [11] H. M. J. Almohri, L. T. Watson, D. Yao, X. Ou, "Security Optimization of Dynamic Networks with Probabilistic Graph Modeling and Linear Programming," *IEEE Trans. Dependable and Secure Computing*, vol. 13, no. 4, pp. 474-487, 2016.
- [12] H. Okhravi, J. Riordan, K. M. Carter, "Quantitative Evaluation of Dynamic Platform Techniques as a Defensive Mechanism," *Lecture Notes in Computer Science*, vol. 8688, pp. 405-425, 2014.
- [13] Z. Hu, M. Zhu, P. Liu, "Online Algorithms for Adaptive Cyber Defense on Bayesian Attack Graphs," in MTD@CCS, pp. 99-109, 2017.
- [14] W. Connell, D. A. Menascé, M. Albanese, "Performance Modeling of Moving Target Defenses," in MTD@CCS, pp. 53-63, 2017.
- [15] N. Anderson, R. Mitchell, I. R. Chen, "Parameterizing Moving Target Defenses," in Int'l Conf. Parameterizing Moving Target Defenses (NTMS'16), pp. 1-6, 2016.
- [16] X. Chang, S. Lv, R. J. Rodríguez, K. Trivedi, "Survivability Model for Security and Dependability Analysis of a Vulnerable Critical System," *IEEE IoTPST*, 2018.

- [17] K. Zaffarano, J. Taylor, S. Hamilton, "A Quantitative Framework for Moving Target Defense Effectiveness Evaluation," in MTD@CCS, pp. 3-10, 2015.
- [18] R. Zhuang, S. Zhang, S. DeLoach, X. Ou, A. Singhal, "Simulation-based approaches to studying effectiveness of moving-target network defense," in Nat'l symp. Moving Target Research (MTR'12), pp. 15111-15126, 2012.
- [19] J. H. Jafarian, E. Al-Shaer, Q. Duan, "Openflow random host mutation: transparent moving target defense using software defined networking," in Proc. HotSDN@SIGCOMM, pp. 127-132, 2012.
- [20] A. Niakanlahiji, J. H. Jafarian, "WebMTD: Defeating Web Code Injection Attacks using Web Element Attribute Mutation," in Proc. MTD@CCS, pp. 17-26, 2017.
- [21] R. Skowrya, K. Bauer, V. Dedhia, H. Okhravi, "Have No PHEAR: Networks Without Identifiers," in Proc. MTD@CCS, pp. 3-14, 2016.
- [22] Y. Wang, Q. Chen, J. Yi, J. Guo, "U-TRI: Unlinkability Through Random Identifier for SDN Network," in Proc. MTD@CCS pp. 3-15, 2017.
- [23] K. M. Carter, J. Riordan, H. Okhravi, "A Game Theoretic Approach to Strategy Determination for Dynamic Platform Defenses," in Proc. MTD@CCS, pp. 21-30, 2014.
- [24] J. B. Hong, S. Yoon, H. Lim, D. S. Kim, "Optimal Network Re-configuration for Software Defined Networks Using Shuffle-Based Online MTD," in IEEE Symp. Reliable Distributed Systems (SRDS'17), pp. 234-243, 2017.
- [25] C. Lei, H. Zhang, L. Wang, L. Liu and D. Ma, "Incomplete information Markov game theoretic approach to strategy generation for moving target defense," *Computer Communications*, vol. 116, pp. 184-199, 2018.
- [26] C. A. Petri, "Kommunikation mit Automaten," Phd Thesis Institut Fuer Instrumentelle Mathematik, 1962.
- [27] J. L. Peterson, "Petri Net Theory and the Modeling of Systems," *Computer Journal*, vol. 25, no. 1, 2010.
- [28] G. Ciardo, A. Blakemore, P. F. C. Jr., J. K. Muppala and K. S. Trivedi, "Automated Generation and Analysis of Markov Reward Models Using Stochastic Reward Nets," Springer New York, 1993.
- [29] G. Ciardo, J. K. Muppala and K. S. Trivedi, "SPNP: Stochastic Petri Net Package," in *Petri Nets and Performance Models (PNPM'89)*, pp. 142-151, 1989.
- [30] "Microsoft Security Bulletin Summary for March 2017," Microsoft, <https://docs.microsoft.com/en-us/security-updates/securitybulletins/summaries/2017/ms17-mar>, Mar. 2017.



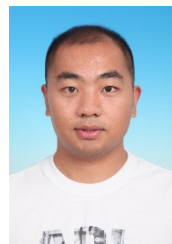
蔡雨彤 于 2017 年在北京交通大学信息安全(保密技术)专业获得学士学位。现在北京交通大学网络空间安全专业攻读硕士学位。研究领域为移动目标防御。Email: 17120466@bjtu.edu.cn



常晓林 于 2005 年在香港科技大学计算机科学技术专业获得博士学位。现任北京交通大学计算机与信息技术学院教授。研究领域包括: 网络空间安全和人工智能安全。Email: xlchang@bjtu.edu.cn



石 禹 于 2017 年在江南大学计算机科学与技术专业获得学士学位。现在北京交通大学网络空间安全专业攻读硕士学位。研究领域为横向渗透攻击、移动目标防御。Email: 17120478@bjtu.edu.cn



陈 志 于 2014 年在北京交通大学信息安全专业获得学士学位。现在北京交通大学信息安全专业攻读博士学位。研究领域为系统安全、移动目标防御。研究兴趣包括: 云计算、网络安全。Email: chenzhi@bjtu.edu.cn