

容器云中基于信号博弈的容器迁移与蜜罐部署策略

李凌书, 邬江兴, 曾威, 刘文彦

(信息工程大学, 河南 郑州 450001)

摘要: SaaS 云中的多租户共存和资源共享模式会带来严重的安全隐患。一方面逻辑上命名空间的软隔离容易被绕过或突破, 另一方面由于共享宿主机操作系统和底层物理资源容易遭受同驻攻击, 对容器云中数据可用性、完整性、机密性产生严重威胁。针对 SaaS 云服务容易遭受容器逃逸、侧信道等同驻攻击的问题, 网络欺骗技术通过隐藏执行体的业务功能和特征属性, 增加云环境的不确定度, 降低攻击的有效性。针对容器易遭受同驻攻击的安全威胁, 结合动态迁移、虚拟蜜罐等安全技术, 研究经济合理的网络欺骗方法降低同驻攻击带来的安全威胁。具体而言, 提出一种基于信号博弈的容器迁移与蜜罐部署策略。依据容器面临的安全威胁分析, 使用容器迁移和蜜罐两种技术作为防御方法, 前者基于移动目标防御的思想提高系统的不可探测性, 后者通过布置诱饵容器或提供虚假服务来迷惑攻击者; 鉴于网络嗅探是网络攻击链的前置步骤, 将攻防过程建模为双人不完全信息的信号博弈, 发送者根据自己类型选择释放一个信号, 接收者仅能够获取到发送者释放的信号, 而不能确定其类型。对这个完全但不完美的信息动态博弈构建博弈树, 设置攻防双方不同策略组合的开销和收益; 对攻防模型进行均衡分析确定最优的欺骗策略。实验结果表明, 所提策略能够有效提高系统安全性, 同时能够降低容器迁移频率和防御开销。

关键词: 云计算; 容器迁移; 蜜罐; 信号博弈

中图分类号: TN915.08

文献标志码: A

DOI: 10.11959/j.issn.2096-109x.2021042

Strategy of container migration and honeypot deployment based on signal game in cloud environment

LI Lingshu, WU Jiangxing, ZENG Wei, LIU Wenyan

Information Engineering University, Zhengzhou 450001, China

Abstract: Multi-tenant coexistence and resource sharing in the SaaS cloud pose serious security risks. On the one hand, soft isolation of logical namespaces is easy to be bypassed or broken. On the other hand, it is easy to be subjected to co-resident attacks due to sharing of the host operating system and underlying physical resources.

收稿日期: 2020-09-22; 修回日期: 2021-01-20

通信作者: 李凌书, lls.ndsc@aliyun.com

基金项目: 国家重点研发计划(2018YFB0804004); 国家自然科学基金(62002383)

Foundation Items: The National Key R&D Program of China (2018YFB0804004), The National Natural Science Foundation of China (62002383)

引用格式: 李凌书, 邬江兴, 曾威, 等. 容器云中基于信号博弈的容器迁移与蜜罐部署策略[J]. 网络与信息安全学报, 2022, 8(3): 87-96.

Citation Format: LI L S, WU J X, ZENG W, et al. Strategy of container migration and honeypot deployment based on signal game in cloud environment[J]. Chinese Journal of Network and Information Security, 2022, 8(3): 87-96.

Therefore it poses a serious threat to data availability, integrity and confidentiality in the container cloud. Given the problem that SaaS cloud services are vulnerable to container escape and side-channel equivalent resident attack, network deception technology increases the uncertainty of the cloud environment and reduces the effectiveness of attack by hiding the business function and characteristic attributes of the executor. Aiming at the security threat caused by the co-resident attack, combining dynamic migration and virtual honeypot security technology, the economical and reasonable network deception method was studied. Specifically, a container migration and honeypot deployment strategy based on the signal game was proposed. According to the security threat analysis, container migration and honeypot were used as defense methods. The former improved the undetectability of the system based on the idea of moving to target defense, while the latter confused attackers by placing decoy containers or providing false services. Furthermore, since network reconnaissance was the pre-step of the network attack chain, the attack and defense process was modeled as a two-person signal game with incomplete information. The sender chose to release a signal according to his type, and the receiver could only obtain the signal released by the sender but could not determine the type. Then, a game tree was constructed for the complete but imperfect information dynamic game, and the costs and benefits of different strategy combinations were set. The optimal deception strategy was determined by equilibrium analysis of attack-defense model. Experimental results show that the proposed strategy can effectively improve system security. Besides, it can also reduce container migration frequency and defense cost.

Keywords: cloud computing, container migration, honeypot, signal game

0 引言

云计算技术将底层基础设施、网络带宽资源以及存储资源通过虚拟化的方式组合成庞大的共享资源池,大量计算任务分布在这些共享资源池上,每个计算任务按需获取所需的计算资源以及存储空间。用户访问上层应用获取想要的服务,而无须知道承载服务运行的具体位置。虚拟化技术在精准地满足用户细粒度需求的同时带来了一定的安全威胁。当多容器共享物理机的虚拟化层,集中存储和集中计算会引发用户数据安全性问题,软件和硬件之间存在附加的抽象层会引起新的安全问题,造成数据泄露、越权访问、拒绝服务、侧信道攻击等威胁^[1]。目前,云环境中与虚拟化技术相关的安全问题已成为业界研究热点。

网络空间安全领域使用欺骗技术可以扭转攻防双方的不对称性,因而受到相关领域安全研究人员的广泛关注。网络欺骗技术通过构造一系列虚假信息误导攻击者的判断,诱导攻击者做出错误的动作^[2]。网络欺骗技术广泛应用于网络攻防,它经常与移动目标防御(MTD, moving target defense)技术相结合,能够以较低的防御成本显著地增加攻击者的攻击难度,使攻击者难以分辨攻击行为是否生效,同时能够详细地记录攻击者

的攻击行为,为之后的防御策略提供一定的依据。近年来网络欺骗技术已成为网络空间防御不可或缺的一部分。Jincent 等^[3]在欺骗环境框架下,结合虚拟云技术和软件定义网络创建了一个实时的、不可预测的且适应性强的欺骗网络。Naagas 等^[4]指出深度防御(DID, defense in depth)无法有效防御复杂的分布式拒绝服务攻击,并将“欺骗防御”和传统防御手段相结合以提高系统的安全性。这些网络欺骗方法可以有效提高网络安全性,但防御者策略往往具有盲目性,难以取得最优的防御效果。

因此,本文提出一种容器云中基于信号博弈的容器迁移与蜜罐部署策略。在该博弈中,当防御者(如系统管理员)接收到防火墙或入侵检测系统(IDS, intrusion detection system)等安全工具的警告时,决定对面临安全风险的容器以一定概率进行迁移,并依据一定的博弈策略释放容器迁移或非迁移的信号。攻击者通过网络侦查和嗅探会接收到这个信号,但不知道目标容器是进行了迁移而发出的真实信号,还是只是一个欺骗性的信号。通过理论推导和实验分析发现,基于信号博弈的容器迁移与蜜罐部署策略可以显著增强云网络的安全性,同时迁移容器的次数少于一般的 MTD 技术,有利于减少云系统开销。

本文的贡献如下。

1) 将欺骗策略建模为一种信号博弈, 并计算攻防双方的均衡策略, 通过分析攻击者的攻击行为和攻击收益, 制定了有效的防御策略。

2) 提出了一种容器云中基于信号博弈的容器迁移与蜜罐部署策略, 通过伪造虚假的容器迁移信号扰乱攻击者, 提高容器云的安全性, 相比单纯的 MTD 技术而言, 可以降低成本。

1 相关工作

随着云计算的飞速发展, 以 Docker 为代表的容器技术逐渐成为云平台搭建中一种主流技术。容器技术可以将单个系统的资源分配到多个相互隔离的组中, 并实现各个组之间资源调度平衡。Docker 提供了一个容器运行轻量化的平台, 它以拓展的 LXC (Linux containers) 来实现轻量级虚拟化, 并通过区分内核名称空间实现容器运行环境的隔离^[5]。容器技术具有与 Linux OS 类似的独立运行管理和配置管理方案, 给云应用程序创造了便利和高速的执行环境, 但是内核共享和独立管理机制意味着将带来了极大的挑战, 威胁着云计算系统的安全性和稳定性, 其重要性和紧迫性不容忽视。

业界对容器和虚拟化技术的安全机制已经进行广泛的研究, 涉及静态预配置、动态威胁防御等方面, 如使用虚拟化层隔离^[6]和安全加固等技术^[7]来隔离容器和虚拟机运行环境, 以防止已知入侵和未知威胁, 然而这些传统的防御方式具有一定的静态性和滞后性。Song 等^[8]提出了一种动态迁移算法来优化大型高级体系结构 (HLA, high level architecture) 系统的运行效率, 同时考虑了通信和迁移成本。Prasad 等^[9]提出了一种用于虚拟机迁移的智能预复制实时迁移方法, 可以最大限度地减少停机时间和迁移时间, 以确保用户服务质量。基于动态防御的理念, 很多学者开始研究基于 MTD 技术保护容器和虚拟机的安全, 将多个虚拟机或容器从一个物理系统环境转移到另一个物理系统环境中以增加不确定性。Zhang 等^[10]提出一种基于激励相容约束 (incentive compatibility constraint) 的移动目标防御策略, 通过定期迁移虚拟机增大攻击者定位目标虚拟机的难度。

Penner^[11]通过随机化虚拟机的位置, 提出一种基于“多臂抽奖” (MAB, multi-armed bandit) 迁移方法来强化云系统安全。Yang 等^[12]提出一种侧信道攻击中的信息泄露模型, 对虚拟机进行迁移以降低信息泄露风险, 建立混合整数线性规划模型求解迁移策略, 实现降低迁移开销和提升防御效果多目标优化。然而, 以上策略由于对攻击者的攻击策略和行为模式的考虑不足, 往往存在盲目调度开销大、策略不能达到最优效果、无法应对高级攻击者等问题。

由于攻防行为相互依存的特性, 博弈论开始广泛应用于网络安全及相关领域, 以制定合理的防御策略。博弈模型充分考虑参与游戏的每一个个体的行为, 并基于此行为分析来研究相关的优化策略。Horák 等^[13]使用博弈论的定量框架研究欺骗行为对攻击者信念的影响, 展示了防御者如何利用这种信念来最大限度地减少攻击者对系统造成的损害。Xiao 等^[14]提出了一种基于进化博弈的部署算法来解决动态虚拟机布局的问题, 并实现能耗优化。Lei 等^[15]通过引入移动攻击面和移动探索面的概念, 扩展了具有单状态或单相不完整信息的移动目标防御的最优策略选择, 提出了一种不完全信息马尔可夫博弈模型来生成最优的 MTD 策略。Adili 等^[16]提出了一种欺骗性应用虚拟机迁移的移动目标防御技术, 通过动态迁移虚拟机降低攻击者成功攻击的概率以提高云计算安全性。冷强等^[17]提出一种基于属性攻击图的网络生存性博弈策略以进行单点防御。

2 威胁分析

云计算系统中的多租户共存和资源共享模式会带来严重的安全隐患, 本文主要针对同驻攻击进行防御。由于容器是共享物理主机内核的, 所有的容器进程在宿主机看来都是由容器进程创建的子进程, 在宿主机上都有相应的进程 ID (PID, process ID), 容器用户创建的进程都建立了独立的名字空间。虚拟化环境下常见的安全威胁如逃逸攻击、侧信道攻击、隔离突破攻击、资源消耗性, 可对容器云中数据可用性、完整性、机密性产生严重威胁。

1) 逃逸攻击。逃逸攻击是指利用虚拟化环境

中软硬件漏洞进行攻击,以实现扰乱或控制虚拟化层或宿主操作系统的目的^[18-19]。容器逃逸攻击一般是指攻击者利用容器和虚拟化平台的交互漏洞发起攻击,交互漏洞通常包括逻辑漏洞和代码缺陷。如果有容器用户通过内核漏洞或潜在的安全问题导致发生 host 逃逸,或者由于误操作导致容器用户提升权限,获得宿主机的超级用户权限,那将对整个宿主机上的容器用户构成威胁。

2) 侧信道攻击。侧信道攻击是当前云环境或数据中心环境下造成多租户间信息泄露的主要原因^[20]。防御侧信道攻击主要有两种方法:第一种方法是直接修改物理主机的软硬件,其可以成功防御特定类型的侧信道攻击,但不适用于防御未知类型的侧信道攻击;第二种方法是基于移动目标防御的思想对容器进行动态迁移,能够成功防御已知和未知的侧信道攻击,不需要直接修改物理主机的软硬件层,但这类方法受限于容器迁移算法的收敛时间和迁移成本开销。

3) 穿透攻击。虽然虚拟化隔离技术尝试阻止位于同一主机的不同容器间的相互干扰,但新的攻击技术不断尝试打破这种隔离。未授权用户存在通过隧道方式连接至其他用户的容器的风险。Docker 提供了一种在容器之间建立虚拟网桥来配置多容器的通信方式。如果攻击者获取了宿主机上其他容器的名字,就可能通过这种方式连接其他容器。

4) 资源消耗性攻击。虚拟机资源消耗攻击是指攻击者通过发送大量恶意请求,将宿主机上的带宽占满并耗尽其网络设备的处理能力,使宿主机无法对其他虚拟机提供正常服务。

3 安全防御技术

本节首先介绍云环境中两种常用的安全防御技术(容器迁移技术和蜜罐技术),进而提出基于这两种安全防御技术的欺骗防御策略。

3.1 容器迁移技术

容器迁移是一种移动目标防御思想的安全技术。容器迁移技术通常可分为冷迁移和热迁移两种形式。冷迁移技术可以细分为无状态迁移和有状态迁移,无状态迁移是指在目标节点生成相同配置的容器环境,有状态迁移是指将当前运行的容

器打包成镜像,再利用该镜像来生成新的容器。目前容器迁移主要实现方式分为3类。

1) 检查点(check point)机制。CRIU 是一个为 Linux 系统提供检查点和恢复检查点的工具,主要是对运行中的应用容器进行冻结,再基于容器在磁盘上的所有文件建立相应的检查点,根据检查点恢复冻结时的容器状态并继续运行。该技术可以应用到容器应用热迁移、快照、远程调试等场景中。

2) 容器镜像迁移。将容器打包成镜像文件,新主机可以通过该镜像文件生成新的容器,并对外提供正常服务。如果镜像文件存储过程使用到数据卷,则迁移过程还需要对相应数据卷进行迁移。集群环境中可以通过建立镜像仓库来共享镜像资源。

3) 利用第三方平台。国内外一些平台和工具(如 flocker 和 jelastic 等)提供了容器实时迁移的服务,但需要依赖于特定的环境。

3.2 蜜罐技术

蜜罐技术广泛应用于网络欺骗防御,它通过布置诱饵主机或提供相关网络服务来迷惑攻击者,诱使攻击者对预先布置的蜜罐进行攻击。蜜罐技术可以通过捕获和分析攻击者的攻击行为,了解攻击者使用的工具和方法,并能够推测出攻击者的攻击意图与目标。蜜罐技术可以分为两种类型:高交互性蜜罐和低交互性蜜罐。低交互性蜜罐模拟一个提供有限的运行条件和信息的生产环境,来引诱攻击者进行攻击;而高交互性蜜罐模拟一个具有高交互功能的运行环境。蜜罐技术经常与其他安全技术协同部署,提高云系统的安全性。

鉴于蜜罐技术在网络安全领域的重要作用,众多学者对其进行了深入研究。Almohannadi 等^[21]在亚马逊云上部署了蜜罐,并通过 Elastic search 技术分析蜜罐日志数据来评估攻击者的行为以发现攻击者的攻击模式。Sarkaler 等^[22]提供了一种基于云容器的主动防御方法,主要用于解决传统的网络防御技术无法快速部署蜜网的问题。Krishnaveni 等^[23]介绍了一种网络体系结构 Honeynet,旨在欺骗攻击者并捕获攻击者的攻击行为特征以进行进一步的分析。Saxena 等^[24]提出

了使用 Kerberos 身份验证系统, 虚拟私有云、虚拟私有网络和弹性文件系统作为云环境中的服务来实现高交互蜜罐的概念, 为云数据提供整体安全性。

3.3 基于欺骗的防御策略

本节以上述两种技术作为防御手段, 提出一种基于欺骗的融合防御方法。所提出的欺骗策略的主要思想是利用虚假信号来迷惑攻击者, 提高网络的安全性, 同时降低防御的成本。当防御者接收到来自防火墙或入侵检测系统的安全警告时, 面临安全风险的容器可能进行迁移以躲避攻击者, 并在迁移前的位置部署蜜罐捕捉攻击者; 防御者也可能为了降低成本而不进行迁移, 但会释放进行了迁移的虚假信息, 并在迁移目的服务器上部署蜜罐。这意味着当容器不迁移时, 仍然有可能使攻击者认为发生了迁移, 诱导攻击者攻击错误的目标。这些虚假信息至少包含以下两方面。

1) 在容器中产生不同的流量行为模拟迁移行为。一个非迁移的容器必须在其当前流量中进行有意的干扰, 让嗅探网络流量的攻击者认为它将会迁移。

2) 当容器不进行迁移时, 在另一台服务器上启动一个同名的容器蜜罐, 声称完成了迁移并提供一个虚假的对外服务接口。当容器进行迁移时, 在原服务器上启动一个同名的容器蜜罐, 并提供一个虚假的对外服务接口。

一个基于信号博弈的容器迁移与蜜罐部署策略实例如图 1 所示。防火墙或入侵检测系统检测到节点 1 上的容器面临恶意攻击, 或节点 1 上有不可信的用户。此时防御者可以将重要的容器迁移到其他服务器上 (如节点 2), 并在节点 1 上启动一个同名的容器蜜罐, 制造出没有进行迁移的假象。防御者也可以进行伪装的迁移, 即真实容器不进行迁移, 但伪造网络流量模拟容器迁移的行为, 并在其他服务器 (如节点 3) 上启动一个同名的容器蜜罐, 制造出进行了迁移的假象。

4 博弈模型与分析

本节首先将容器云中容器迁移与蜜罐部署问

题建模为一个信号博弈模型, 然后对该博弈进行均衡分析, 最后提出最优的欺骗策略。

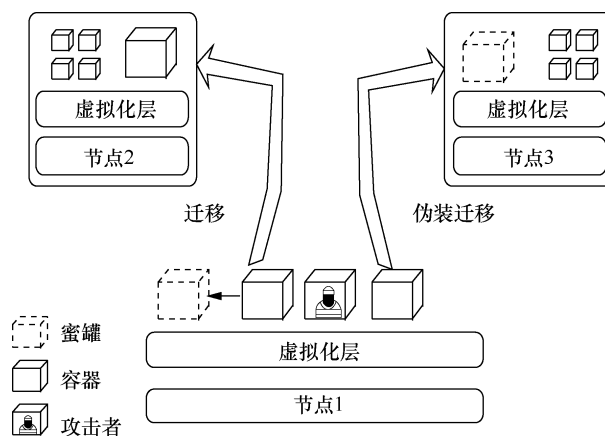


图 1 基于欺骗的安全防御方法
Figure 1 Security defense method based on deception

4.1 博弈模型

信号博弈是一个双人不完整信息博弈, 分别为发送者 S 和接收者 R 。在信号博弈中, 自然 (nature) 会根据预设的分布为发送者选择一个类型 (type), 发送者知道自己类型并发送一个信号。信号类型有迁移 (migration) 和不迁移 (not migration) 两种, 分别表示为 M 和 NM 。接收者不知道发送者的类型, 但能够观察到发送者发送的信号。信号博弈模型 G_{cm} 如图 2 所示, 其中 $p = p(\theta|M)$, $q = q(\theta|NM)$ 。

1) 提供威胁告警的入侵检测系统是自然的, 即入侵检测系统决定网络防御者的类型。自然通过概率 θ 和 $1-\theta$ 决定类型 t_1 或 t_2 。

- ① 如果自然选择 t_1 , 代表系统进行容器迁移。
- ② 如果自然选择 t_2 , 代表系统不进行迁移。

2) 网络防御者根据自身的类型, 决定是否进行伪装, 并发送适当的信号 (真实信号或虚假信号)。

3) 攻击者观察防御者是否释放迁移信号, 但不知道该防御者是在进行真实的迁移, 还是只是模拟迁移。

4) 攻击者有 3 种策略。

- ① a_0 : 攻击者不进行攻击;
- ② a_1 : 攻击者认为目标容器没有迁移, 并发起攻击;
- ③ a_2 : 攻击者认为目标容器进行了迁移, 并

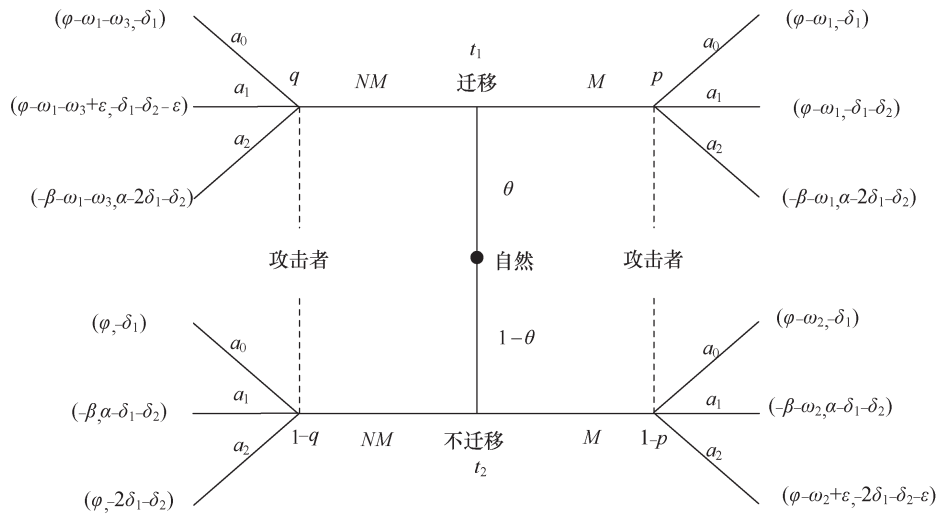


图 2 信号博弈模型
Figure 2 Signal game model

发起攻击。

图 2 所示的博弈是一个完全但不完美信息动态博弈。虚线表示了攻击的信息集，信息集指的是博弈中玩家的决策节点，表示第二个参与者在不知道第一个参与者如何选择的情况下做出选择。

假定 ω_1 代表迁移的成本， ω_2 代表容器不迁移时模拟迁移的开销， ω_3 代表容器迁移时模拟不迁移的开销， φ 代表容器的防御者保护容器不受攻击的收益。 δ_1 攻击成本 1（重新开始扫描、窃听等）。 δ_2 代表攻击成本 2（如进一步进行木马注入）。如果攻击者放弃攻击，只需要付出 δ_1 ；如果选择攻击，需要付出 $\delta_1 + \delta_2$ 。本文使用的主要数学符号及其含义如表 1 所示。

4.2 博弈均衡分析

本节分析信号博弈的任何纯策略完美贝叶斯纳什均衡（PBE, perfect bayesian equilibrium）的存在性和性质。若博弈中玩家的策略组合与各自判断符合以下条件，则称为一个 PBE。

1) 进行选择的博弈方在每个信息集处，具有一个关于博弈到达该信息集中每个节点可能性的信念（belief）。

2) 博弈方基于“序列理性”进行决策。即博弈方在选择当前阶段策略及后续阶段策略时，决策依据都是期望收益最大化。

3) 对于均衡路径上的每一个信息集，信念由贝叶斯法则和各博弈方的均衡策略决定。

表 1 主要数学符号及其含义

Table 1 Mathematical symbols and their meanings

数学符号	含义
θ	IDS 检测到威胁的概率（自然）
M	防御者对容器进行迁移
NM	防御者不对容器进行迁移
a_1	攻击者认为目标容器没有迁移，并发起攻击
a_2	攻击者认为目标容器进行了迁移，并发起攻击
a_0	攻击者不进行攻击
ω_1	容器迁移的开销
ω_2	容器不迁移时，模拟迁移行为的开销
ω_3	容器迁移时，模拟不迁移行为的开销
δ_1	攻击者进行扫描、窃听等开销
δ_2	攻击者进行木马注入后，攻击的开销
φ	防御者保护容器不受攻击的收益
ε	当攻击者攻击蜜罐时，防御者获得的额外收益
β	防御者未能成功保护容器的损失
α	攻击者成功攻击目标容器的收益

4) 对于非均衡路径上的信息集，信念由贝叶斯法则和各博弈方在此处可能的均衡策略决定。

本文使用 $(p, 1-p)$ 和 $(q, 1-q)$ 来表示攻击者在两个信息集中的信念。对于图 2 中定义的信号博弈，防御者的纯策略由一个有序对 $(m(t_1), m(t_2))$ 决定，其中 $m(t_1)$ 是 t_1 选择的策略， $m(t_2)$ 是 t_2 选择的策略。同样，攻击者策略由有序对 $(a(M), a(NM))$

决定, 其中 $a(M)$ 和 $a(NM)$ 分别为根据防御者信号制定的攻击策略。

纯策略 PBE 可以表示为元组 $\{S_D, S_A, p, q\}$, 其中, S_D 是防御者根据每种类型选择信号的策略, S_A 是响应每个信号的攻击者策略对, p 和 q 分别为攻击者发送方类型的信念。发送方采用纯策略的情况下, 信号博弈中可能存在两种类型的 PBE, 称为混同均衡和分离均衡。

当 $m(t_1)=m(t_2)$ 时, PBE 称为混同均衡。换言之, 无论防御者的类型如何, 都会发出相同的信号。相反, PBE 被称为分离均衡, 即防御者根据其类型发出不同的信号。

4.2.1 分离均衡

假设 1 在现实场景中, 一般容器的价值高于迁移的代价, 为简化分析, 本文假定 $\varphi > \omega_i$ 。

假设 2 容器的价值高于攻击开销 ($\alpha > \delta_i$), 否则攻击者会失去攻击意愿。

(1) 若分离均衡为 (M, NM)

根据假设 2, 由于 $\alpha > \delta_2$, 攻击者的最优策略是 (a_2, a_1) , 此时判断防御者会不会偏离: t_2 状态的防御者会不选择 NM 而选择 M , 来获取更大的收益 (根据假设 1, $\varphi - \omega_2 + \varepsilon + \beta > 0$), 因此不存在分离均衡 (M, NM) 。

(2) 若分离均衡为 (NM, M)

此时攻击者的最优策略是 (a_2, a_1) 。 t_1 状态的防御者会不选择 NM 而选择 M , 来获取 $\varphi - \omega_1 + \varepsilon$ 的收益, 收益大于 $-\beta - \omega_1 - \omega_3$, 故不存在分离均衡 (NM, M) 。

4.2.2 混同均衡 (M, M)

若防御策略为 (M, M) , 攻击者在该信息集的信念为 $(q, 1-q)$ 。由于 $p(M|t_1) = p(M|t_2) = 1$, 由贝叶斯公式可得 $p = p(M|t_1) = p(t_1) = \theta$ 。

攻击者选择 a_0 的收益期望为 $C_0 = \theta(-\delta_1) + (1-\theta)(-\delta_1)$; 攻击者选择 a_1 的收益期望为 $C_1 = \theta(-\delta_1 - \delta_2) + (1-\theta)(\alpha - \delta_1 - \delta_2)$; 攻击者选择 a_2 的收益期望为 $C_2 = \theta(\alpha - 2\delta_1 - \delta_2) + (1-\theta)(-2\delta_1 - \delta_2)$ 。令 $C_1 - C_0 = \theta(-\delta_2) + (1-\theta)(\alpha - \delta_2) = (1-\theta)\alpha - \delta_2 > 0$, 则相当于 $\theta < 1 - \delta_2 / \alpha$ 时, $C_1 > C_0$ 。

同理, 当 $\theta > \frac{(\delta_1 + \delta_2)}{\alpha}$ 时, $C_2 > C_0$; 当

$\theta > \frac{\alpha + \delta_1}{2\alpha}$ 时, $C_2 > C_1$ 。

总结如下。

1) 当 $\theta > 1 - \frac{\delta_2}{\alpha}$ 且 $\theta < \frac{(\delta_1 + \delta_2)}{\alpha}$ 时, 攻击者选 a_0 。

2) 当 $\theta < \frac{\alpha + \delta_1}{2\alpha}$ 且 $\theta < 1 - \frac{\delta_2}{\alpha}$ 时, 攻击者选 a_1 。

3) 当 $\theta > \frac{\alpha + \delta_1}{2\alpha}$ 且 $\theta > \frac{(\delta_1 + \delta_2)}{\alpha}$ 时, 攻击者选 a_2 。

攻击者选 a_0 时, 要确定两种防御者类型是否都愿意选择 M , 本文需要观察攻击者对 NM 的反应。如果攻击者选择策略 a_0 , 类型为 t_2 的防御者会选择 NM 来获取 φ 的收益, 高于选择 M 的 $\varphi - \omega_2$ 。

攻击者选 a_1 时, 要确定两种防御者类型是否都愿意选择 M , 本文需要观察攻击者对 NM 的反应。如果攻击者选择策略 a_1 , 类型为 t_2 的防御者会选择 NM 来获取 $-\beta$ 的收益, 高于选择 M 的 $-\beta - \omega_2$ 。

攻击者选 a_2 时, 要确定两种防御者类型是否都愿意选择 M , 需要观察攻击者对 NM 的反应。当 $\varepsilon < \omega_2$ 时, 如攻击者选择策略 a_2 , 类型为 t_2 的防御者都选择 NM 。当 $\varepsilon > \omega_2$ 时, 如攻击者选择策略 a_2 , 类型为 t_1 和 t_2 的防御者都不会选择 NM 。因此, (M, M) 存在混同均衡 $\{(M, M), (a_2, a_2), p = \theta, q\}$ 。

4.2.3 混同均衡 (NM, NM)

若防御策略为 (NM, NM) , 攻击者在该信息集的信念为 $(q, 1-q)$ 。由于 $p(NM|t_1) = p(NM|t_2) = 1$, 因此由贝叶斯公式可得 $q = p(NM|t_1) = p(t_1) = \theta$ 。

攻击者选择 a_0 的收益期望为 $C_0 = \theta(-\delta_1) + (1-\theta)(-\delta_1)$; 攻击者选择 a_1 的收益期望为 $C_1 = \theta(-\delta_1 - \delta_2) + (1-\theta)(\alpha - \delta_1 - \delta_2)$; 攻击者选择 a_2 的收益期望为 $\theta(\alpha - 2\delta_1 - \delta_2) + (1-\theta)(-2\delta_1 - \delta_2)$ 。

1) 当 $\theta > 1 - \frac{\delta_2}{\alpha}$ 且 $\theta < \frac{(\delta_1 + \delta_2)}{\alpha}$ 时, 攻击者选 a_0 。

2) 当 $\theta < \frac{\alpha + \delta_1}{2\alpha}$ 且 $\theta < 1 - \frac{\delta_2}{\alpha}$ 时, 攻击者选 a_1 。

3) 当 $\theta > \frac{\alpha + \delta_1}{2\alpha}$ 且 $\theta > \frac{(\delta_1 + \delta_2)}{\alpha}$ 时, 攻击者选 a_2 。

攻击者选 a_0 时, 要确定两种防御者类型是否都愿意选择 NM , 本文需要观察攻击者对 M 的反应。如果攻击者选择策略 a_0 , 类型为 t_1 的防御者会选择 M 来获取 $\varphi - \omega_1$ 的收益, 高于选择 NM 的 $\varphi - \omega_1 - \omega_3$ 。

攻击者选 a_1 时, 要确定两种防御者类型是否都愿意选择 NM , 本文需要观察攻击者对 M 的反应。当 $\varepsilon < \omega_3$ 时, 如果攻击者选择策略 a_1 , 类型为 t_1 的防御者会选择 M 来获取 $\varphi - \omega_1$ 的收益, 高于选择 NM 的 $\varphi - \omega_1 - \omega_3 + \varepsilon$ 。当 $\varepsilon > \omega_3$ 时, 如果攻击者选择策略 a_1 , 类型为 t_1 和 t_2 的防御者都不会选择 M 。因此存在混同均衡 $\{(NM, NM), (a_1, a_1), p, q = \theta\}$ 。

攻击者选 a_2 时, 要确定两种防御者类型是否都愿意选择 NM , 本文需要观察攻击者对 M 的反应。如果攻击者选择策略 a_2 , 类型为 t_1 的防御者会选择 M 来获取 $-\beta - \omega_1$ 的收益, 高于选择 NM 的 $-\beta - \omega_1 - \omega_3$ 。

5 实验

为评估欺骗模型的可行性及博弈算法有效性, 本节将迁移、欺骗开销和安全价值综合为攻防双方的收益来进行对比, 对不同攻防策略组合进行实验分析。

5.1 环境与参数设置

测试网络环境包括 4 台 x86 服务器 (28 cores 2.00GHz, 256GB RAM, 10 GB NIC), 其中 1 台为控制节点, 3 台为计算节点。采用 Kubernetes 作为管理与编排系统对容器进行管理, 使用 CRUI 技术对容器进行迁移, 基于开源的 Opencanary 蜜罐系统实现相关蜜罐的部署。从可用性、完整性、机密性 3 个方面评估容器的价值, 攻击成功会破

坏容器的机密性, 容器迁移、蜜罐部署会消耗资源, 并降低可用性。

对于实验参数设置, 本文假定符合表 2 中完美贝叶斯纳什均衡的存在条件 ($\varepsilon > \omega_2$, $\varepsilon > \omega_3$)。 ε 表示当攻击者攻击蜜罐时, 防御者因捕获到攻击行为而获得的额外收益。 ω_2 表示容器不迁移时, 模拟迁移行为的开销, ω_3 表示容器迁移时, 模拟不迁移行为的开销。这两个约束条件在一般情况下是成立的, 即捕获攻击的收益大于进行网络欺骗的开销。对于其他开销的取值, 与攻防双方的技术能力以及网络设备价值有关, 但实际上不影响均衡点的位置, 也不影响最终的策略选择。因此实验参数设置为 $\alpha = 10$, $\delta_1 = 1$, $\delta_2 = 1$, $\omega_1 = 4$, $\omega_2 = 3$, $\omega_3 = 2$, $\varepsilon = 4$, $\varphi = 10$, $\beta = 4$ 。

假定攻击者具有两类攻击模式: 一类是随机攻击模式, 其无论接收到什么类型的信号, 均采取随机攻击; 另一类是最优攻击模式, 其根据接收到的防御者发出信号做出不同的选择。如当收到非迁移信号 NM 时选择攻击原服务器 a_1 , 当收到迁移信号 M 时选择攻击迁移目的服务器 a_2 , 记为 (a_1, a_2) 。因此, 其攻击策略集合包含 9 种策略。此类模式下攻击者具有很强的记忆和试错能力, 能够选择最优的策略进行攻击。

防御者也假定有两类防御模式: 一类是随机防御模式, 其无论容器实际是否迁移 (无论自己的类型是 t_1 还是 t_2), 都随机释放一个信号; 另一类是博弈防御模式, 其根据当前系统容器迁移的概率 θ , 选择相应的防御策略, 即对于迁移和非迁移情况下释放什么信号, 其防御策略集合包含 4 种策略。策略选择依据表 2 进行计算。

5.2 实验结果与分析

根据攻击者和防御者模式的假设, 共有 4 种攻防组合。不同攻防组合下的平均收益如图 3 所示。可以看出, 无论防御者采用何种防御模式, 最优攻击模式下攻击者均具有更强的攻击能力, 可以

表 2 G_{cm} 的完美贝叶斯纳什均衡
Table 2 Perfect Bayesian Nash equilibrium G_{cm}

编号	G_{cm} 参数要求	θ 的取值范围	PBE
PBE1	$\varepsilon > \omega_2$	$\left[\max\left(\frac{(\delta_1 + \delta_2)}{\alpha}, \frac{\alpha + \delta_1}{2\alpha}\right), 1 \right]$	$\{(M, M), (a_2, a_2), p = \theta, q\}$
PBE2	$\varepsilon > \omega_3$	$\left[0, \min\left(\frac{\alpha + \delta_1}{2\alpha}, 1 - \frac{\delta_2}{\alpha}\right) \right]$	$\{(NM, NM), (a_1, a_1), p, q = \theta\}$

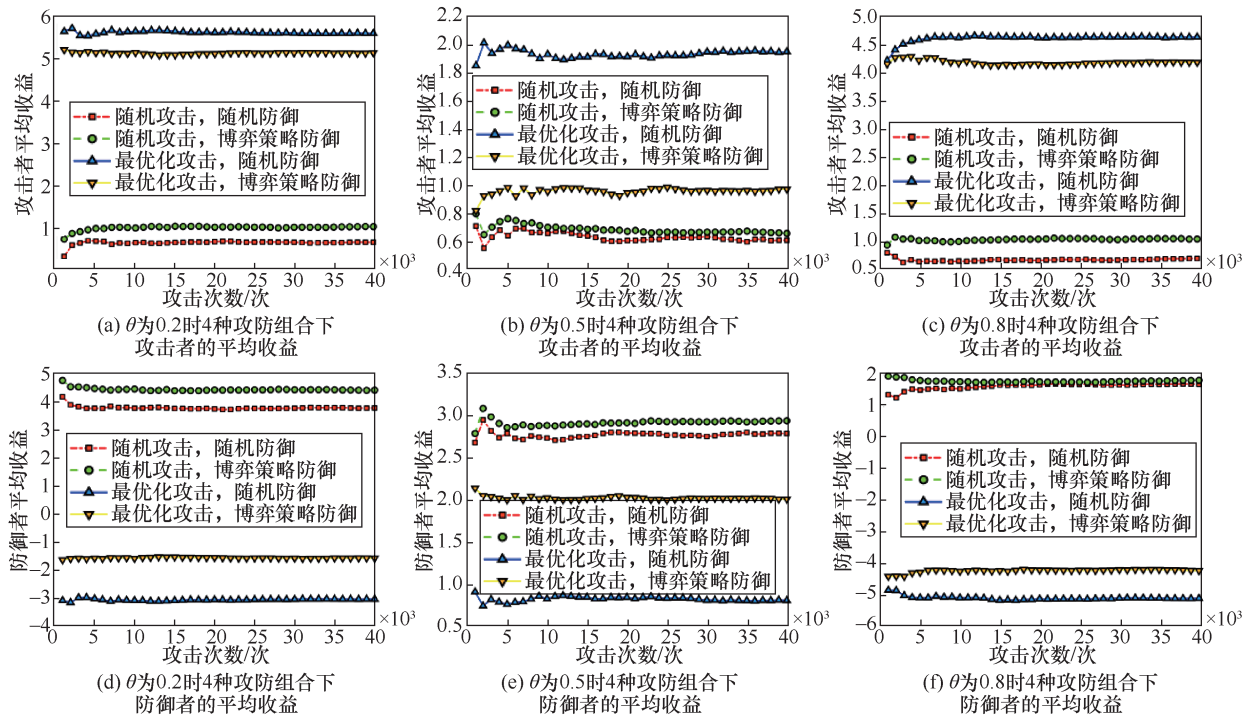


图3 不同攻防组合下的平均收益
Figure 3 Average payoffs of different attack and defense combinations

获得更好的攻击收益。同时, 无论攻击者采用何种攻击模式, 博弈策略防御模式下的防御者均能获得更好的防御收益, 验证了博弈算法的有效性。由于攻击者能力强, 具有后手优势, 倾向于使用最优化攻击, 防御者必须考虑最坏攻防情况下的策略选择, 因此最终会选择均衡策略。当达到均衡点之后, 攻防双方均没有意愿改变策略来偏离均衡点。当 θ 为0.2, 0.5时, 均衡为 $\{(NM, NM), (a1, a1), p, q=\theta\}$ 。即防御者选择释放不迁移的信号, 攻击者选择攻击原宿主服务器。当 θ 为0.8时, 均衡为 $\{(M, M), (a2, a2), p=\theta, q\}$ 。即防御者选择释放迁移的信号, 攻击者选择攻击容器迁移的目标服务器。

通过对攻防信号博弈模型的均衡和数据进行一般性分析, 可以得到以下规律。

1) 防御者释放的信号倾向于与其类型保持一致。即 θ 越大, 防御者是 M 的类型概率越高, 释放 M 信号的概率越大。即 θ 越小, 防御者是 NM 的类型概率越高, 释放 NM 信号的概率越大。这是因为释放虚假信号需要付出代价, 防御者倾向于降低不必要的欺骗开销。

2) 攻击者倾向于相信防御者释放的信号。这意味着当防御者释放假信号时, 能够成功欺骗攻击者, 从而获得更大的收益, 证明了欺骗策略的有效性。

3) 防御者应尽可能避免分离均衡。如果防御者在不同类型的情况下释放不同的信号, 则攻击者可以准确地判断防御者是否进行迁移, 无法达到扰乱攻击者的目的。防御者释放的信号应具有不确定性, 否则容易被高级攻击者识破, 如使用简单的虚拟IP技术虽然能够隐藏真实IP, 如果不进行周期性的跳变, 攻击者依然能通过虚拟IP定位到目标主机。

6 结束语

本文将移动目标防御技术与网络欺骗相结合, 提出了一种基于信号博弈的容器迁移与蜜罐部署策略, 该策略利用容器迁移和蜜罐部署的不确定性来增加系统安全性。本文将攻防过程建模为一个主从信号博弈, 防御者作为领导者释放迁移信号, 攻击者作为跟随者通过网络嗅探获取攻击者的信号, 再选取相应的攻击策略。通过博弈均衡分析求解了防御者和攻击者的均衡策略, 本文据此得出了防御者最优的容器迁移欺骗策略。容器云的资源灵活配置的特点有利于部署蜜罐和一些移动目标防御策略, 但开销依然是亟待解决的问题, 本文利用网络欺骗降低容器被攻击的概率, 提高蜜罐捕获攻击的可能性, 可以有效提高信息系统的安全性, 同时降低防御成本。

参考文献:

- [1] JITHIN R, CHANDRAN P. Virtual machine isolation[C]//International Conference on Security in Computer Networks and Distributed Systems, 2014.
- [2] JAJODIA S, SUBRAHMANYAN V S, SWARUP V, et al. Cyber deception[R]. 2016.
- [3] VINCENT E U. Computer network deception as a moving target defense[C]//2015 International Carnahan Conference on Security Technology (ICCST), 2015: 1-6.
- [4] NAAGAS M A. Defense-through-deception network security model: securing university campus network from DoS/DDoS attack[J]. Bulletin of Electrical Engineering and Informatics, 2018: 593-600.
- [5] SI-YAO L, QIANG L I, BIN L I. Research on isolation of container based on docker technology[J]. Computer Engineering & Software, 2015.
- [6] ZHENG Z. Virtual machine security isolation and protection based on cloud platform[J]. China Computer & Communication, 2018.
- [7] ABDELRAHEM O, BAHAA-ELDIN A M, TAHA A. Virtualization security: a survey[C]//International Conference on Computer Engineering & Systems. 2017.
- [8] SONG X, MA Y, TENG D. A load balancing scheme using federate migration based on virtual machines for cloud simulations[J]. Mathematical Problems in Engineering, 2015, 5: 1-11.
- [9] PRASAD T S, MALLIKARJUNA A, RAMAKRISHNA S. From cloud to fog computing: a review and a conceptual live VM migration framework[J]. IEEE Access, 2017, 99:1-1.
- [10] ZHANG Y, LI M, BAI K, et al. Incentive compatible moving target defense against VM-colocation attacks in clouds[C]//IFIP International Information Security Conference. 2012.
- [11] PENNER T, GUIRGUIS M. Combating the bandits in the cloud: a moving target defense approach[C]//IEEE/ACM International Symposium on Cluster, 2017.
- [12] YANG C, GUO Y, HU H, et al. An effective and scalable VM migration strategy to mitigate cross-VM side-channel attacks in cloud[J]. Networks & Security, 2019: 151-171.
- [13] HORÁK K. Manipulating adversary's belief: a dynamic game approach to deception by design for proactive network security[C]//8th International Conference on Decision and Game Theory for Security. 2017: 273-294.
- [14] XIAO Z, JIANG J, ZHU Y, et al. A solution of dynamic VMs placement problem for energy consumption optimization based on evolutionary game theory[J]. Journal of Systems & Software, 2015, 101(3): 260-272.
- [15] LEI C, ZHANG H Q, WAN L M, et al. Incomplete information markov game theoretic approach to strategy generation for moving target defense[J]. Computer Communications, 2018, 116(1): 184-199.
- [16] ADILI M T, MOHAMMADI A, MANSHAEI M H, et al. A cost-effective security management for clouds: a game-theoretic deception mechanism[C]//Integrated Network & Service Management. 2017: 98-106.
- [17] 冷强, 杨英杰, 常德显, 等. 面向网络实时对抗的动态防御决策方法[J]. 网络与信息安全学报, 2019, 5(6): 58-66.
- [18] LENG Q, YANG Y J, CHANG D X, et al. Dynamic defense decision method for network real-time confrontation[J]. Chinese Journal of Network and Information Security, 2019, 5(6): 58-66.
- [19] ALNAIM A, ALWAKEEL A, FERNANDEZ E B. A misuse pattern for compromising VMs via virtual machine escape in NFV[C]//The 14th International Conference. 2019.
- [20] KOCHER P. Spectre attacks: exploiting speculative execution[J]. Communications of the ACM, 2018.
- [21] ALMOHANNADI H. Cyber threat intelligence from honeypot data using elasticsearch[C]//2018 IEEE 32nd International Conference on Advanced Information Networking and Applications (AINA). 2018: 900-906.
- [22] SARKALE V V, RAD P, LEE W. Secure cloud container: runtime behavior monitoring using most privileged container (MPC)[C]//IEEE International Conference on Cyber Security & Cloud Computing. 2017.
- [23] KRISHNAVENI S, PRABAKARAN S, SIVAMOCHAN S. A survey on honeypot and honeynet systems for intrusion detection in cloud environment[J]. Journal of Computational and Theoretical Nanoence, 2018.
- [24] SAXENA A. Virtual public cloud model in honeypot for data security: a new technique[C]//5th International Conference on Computing and Artificial Intelligence. 2019: 66-71.

[作者简介]



李凌书 (1992-), 男, 湖北恩施人, 信息工程大学博士生, 主要研究方向为拟态安全防御、网络欺骗。



邬江兴 (1953-), 男, 浙江嘉兴人, 中国工程院院士, 信息工程大学教授、博士生导师, 主要研究方向为拟态安全防御、内生安全防御。



曾威 (1997-), 男, 河南信阳人, 信息工程大学硕士生, 主要研究方向为移动目标防御、云资源管理与调度。



刘文彦 (1986-), 男, 河南周口人, 信息工程大学讲师, 主要研究方向为云计算、网络功能虚拟化、云资源管理与调度。