操作系统行为理论模型及典型应用研究

祝　林，邬　江，刘克斌，钟　杰
（中电长城网际安全技术研究院（北京）有限公司，北京　100097）

摘　要：针对当前终端网络安全攻防对抗中未知攻击“防不住”、已知攻击“测不准”的问题，现用“封堵管控”安全机制可被攻击方屏蔽规避，为扭转当前终端安全防护的被动落后现状，亟需在终端安全检测理论、安全检测分析模型与实际应用上实现创新突破。文章将操作系统行为进行了形式化定义，并基于形式化定义设计了操作系统行为分析模型，然后以缓冲区溢出攻击与终端数据泄露攻击为典型示例验证其方法正确性。

关键词：行为测量；操作系统行为；安全检测；终端防护
中图分类号：TP309；TP391　　**文献标识码：**A　　**DOI：**10.19358/j.issn.2097-1788.2024.12.004
引用格式：祝林，邬江，刘克斌，等. 操作系统行为理论模型及典型应用研究［J］. 网络安全与数据治理，2024，43（12）：27-32.

Research on the theory and typical applications of operating system behavior

Zhu Lin，Wu Jiang，Liu Kebin，Zhong Jie
（CLP Great Wall Internet Security Technology Research Institute（Beijing）Co.，Ltd.，Beijing 100097，China）

Abstract：In response to the problem of unknown attacks being "undetectable" and known attacks being "unpredictable" in current terminal network security attacks and defenses，the current "blocking and control" security mechanism can be blocked or avoided by attackers. In order to reverse the passive backwardness of terminal security protection，it is needful to achieve innovative breakthroughs in terminal security detection theory，security detection analysis models，and practical applications. This study formalized the behavior of the operating system and designed an operating system behavior analysis model based on the formal definition. Then，buffer overflow attacks and terminal data leakage attacks were used as typical examples to verify the correctness of the method.

Key words：behavior measurement；operating system behavior；security testing；terminal protection

0　引言

为应对常见的安全风险（如非法访问、网络恶意攻击、网络数据泄露、网络病毒、非法外联、违规外设接入、勒索软件、终端非授权使用等），往往会针对性部署防火墙、主机入侵检测/入侵防御系统、终端检测和响应[1]（Endpoint Detection and Response，EDR）、恶意代码查杀、主机安全管理系统、主机外设管控系统、基于电子钥匙的身份认证等安全措施。

当前安全防护措施的处置过程，以网络数据泄露为例，如图1所示，主要包括：

（1）针对安全风险（已知漏洞）；

（2）部署安全措施（特征匹配、主动检测）；

（3）检测发现安全事件；

（4）安全响应处置。

现有安全防护机制是典型的以现象和结果作为切入点，其存在如下问题：一是始终无法有效防范APT[2]攻击，特别是对基于0-day漏洞[3]的未知攻击往往无法实现有效防护；二是多重安全机制导致防护性能低下，已影响当前安全产品广泛应用推广；三是多维度安全检测数据难以融合分析，异构安全数据的关联分析一直是困扰安全检测有效性与准确性的核心理论问题；四是安全检测与攻击规避对立问题[4]，当前安全检测未充分考虑攻击规避对抗，导致检测措施可被攻击方规避绕过[5]，从而造成检测失效。

从目前攻防对抗发展趋势来看，安全风险的“日新月异”导致安全防护的“无边扩展”，而这种应对式无序发展，造成的结果就是终端上安全软件堆砌、安全防护系统整体运行效能低下，终端安全对抗一直处于“道高一寸，魔高一尺”的追赶局面。

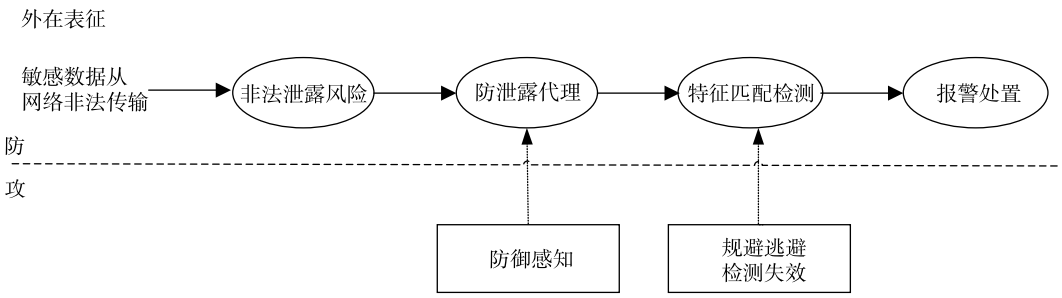

图 1　以数据泄露为例当前攻防检测与反制措施分析

其产生的原因在于：目前安全防护机制是“以现象为切入、以工程思维进行分析、亡羊补牢式的”安全防护。本文针对当前安全防护“头痛医头，脚痛医脚”、治标不治本、未从安全防护本质上来解决问题的不足，从安全攻防内在机理上进行溯源分析，从根本上分析安全威胁的成因。即要克服现有终端安全机制的弊端，需要转变方法思路，从清本溯源角度来解决终端安全防护问题。

1　相关研究

1.1　传统安全防护系统分析

传统的安全防护手段主要有以下几种：

（1）防病毒软件

传统防病毒软件主要有两类实现方式：静态防护和动态防护。静态防护的基本原理是依托已知病毒代码特征，通过对磁盘文件及内存数据段进行实时扫描，并对待检测代码计算后提取其特征值，与已知特征库比对，最终实现恶意代码的判定。在实现上，静态防护监测范围对象主要为磁盘文件和实时内存数据区，其往往以代理方式实现部署。动态防护主要是对操作系统内部调用，特别是系统调用进行监控。通常以代理方式部署在内核中实现，实时获取运行中系统调用及相关参数，并将监测调用及参数作为特征进行分析比对。从实现上可以发现动态分析监测范围对象主要为系统调用。

（2）主机防火墙

主机防火墙通常通过在目标主机上部署代理程序来隔断非法进出终端的网络流量，其监测范围包括网络流量与相关应用层传输数据等。通过在操作系统内核中实时监测网络系统调用来实现其监测机制，同时结合采集的应用层数据进行特征匹配，进而实现应用层防病毒的检测。

（3）端点检测和响应（EDR）

EDR 是一种整套终端安全解决方案，旨在通过在目标主机上运行代理程序，使用实时分析和记录应用程序各种操作动作，并通过多种数据分析技术检测可疑操作动作，以阻止恶意行为并为受影响的主机终端系统提供修复建议。EDR 安全解决方案通过在每个端点设备上安装轻量级数据收集工具或代理来实现。

（4）终端安全加固[6]

终端安全加固通过修改内核模块从而提高主机操作系统的安全性和抗攻击能力，以减少安全风险，确保主机操作系统正常运行和业务系统正常工作。

内核加固技术可通过安全标记来判断用户是否具有访问和控制权限，通过身份认证、强制访问控制、进程保护和网络强制访问控制等机制，确保终端系统安全。内核加固往往在内核中部署，通过动态加载模块方式运行。

对上述安全防护系统进行综合分析（见表 1），可以发现当前防护系统一般都是以代理方式部署，其工作往往在操作系统内核层（攻击系统也部署在该层），这种攻防同层部署实现机制下仅能实现对其他应用的观察（无法保证真实有效），因为其监测到的相关数据有可能被恶意程序欺骗或篡改。

表 1　当前安全防护系统监测数据对象表

	防病毒软件	主机防火墙	EDR	终端安全加固
内存数据	√	×	√	√
OS 配置数据	√	×	√	×
系统调用	√	×	√	√
系统日志	×	×	√	×
文件系统	√	×	√	√
系统进程	×	×	×	×
网络流量	×	√	√	×
内核模块	×	×	√	√

1.2　操作系统行为理论相关研究

在计算机终端事件与操作的研究方面，文献［7］将虚拟机状态变化和事件行为定义为虚拟机操作系统行为。文献［8］对基于系统调用的主机异常检测的研究现状进行了梳理，分析和对比了系统调用异常检测常用算法和模型，并介绍了异常检测常用的评估指标。文献［9］探

讨了深度学习算法和模型在操作系统的行为和性能方面的应用，对比了用户态与内核态中实现机制特点与优缺点，提出了一种基于 Keras 的深度学习内核模块编译方法。文献［10］分析了在安全防护领域引入大数据分析的必要性，在数据存储、检索、分析方面探讨了大数据技术的应用，并对典型攻击场景的关联分析进行阐述。

基于上述研究，本文拟提出操作系统行为的有效描述方法，将大数据分析方法引入操作系统安全分析，设计了操作系统行为分析模型并验证其正确性。

2 操作系统行为

操作系统行为是指操作系统在执行其功能和任务时所进行的各种活动和操作，包括资源管理、进程管理、内存管理、设备管理与网络通信等，并且依赖这些行为组合协作实现了操作系统的核心功能和相关应用任务。本文拟通过深入研究操作系统行为，探索基于操作系统行为分析基础上的分析检测方法。综合已有研究，将各种操作系统的动作通过统一的形式化方式实现描述。

2.1 操作系统行为形式化定义

将操作系统行为以（P，O，A，D，R，→）进行定义描述，其中：

（1）P 代表操作的主体集合，$p_{id} \in P$，其中 p_{id} 表示某个具体主体（进程或线程），id 为该进程的进程号（线程号），其为一个操作系统的唯一标识；

（2）O 代表操作的客体集合，$o_{name} \in O$，o_{name} 代表某个具体对象，name 为客体名称；

（3）A 代表操作系统行为运行集，$a_{name} \in A$，a_{name} 代表某个具体动作，name 为具体动作名称；

（4）D 代表执行动作需要的数据参数（可选），$d_n \in D$，d_n 代表某个相关数据；

（5）R 代表动作执行结果或输出，$r_n \in R$，r_n 代表某个相关数据；

（6）→代表映射关系，p，o，a，$d \rightarrow r$ 代表某一主体 p 对某一客体 o 执行动作 a 后（含相关参数 d 输入）得到（映射）相应运行结果 r。

相关函数定义说明如下：

（1）$p_{id} \in P$，类型属性 $P_{type}|p_{id}|$ = {0 代表系统进程；1 代表应用进程；2 代表线程}；地址空间 Memzone $|p_{id}|$ = {Low 代表分配地址空间下限；High 代表分配地址空间上限}；

（2）主体的权限函数 $\mathrm{Pr}|p_{id}|$ = {可执行操作列表}；

（3）客体 o_{name} 的客体属性函数 $O_{type}|o_{name}|$ = {0 代表进程；1 代表内存；2 代表文件；3 代表网络通信；4 代表信号；5 代表块设备；6 代表字符设备}。

2.2 操作系统行为对象

操作系统行为的主体定义为操作系统内运行的实体，如进程或线程，具体可以分为系统进程、用户进程与线程 3 类。而这些主体还具有相关属性，包括地址空间与运行权限，地址空间是运行的进程或线程分配的可用内存地址范围；运行权限是主体实际可执行操作的范围，即其拥有权限运行的操作集。

操作系统行为的客体是主体实施操作的对象，其由进程、内存、文件、网络通信、信号、块设备、字符设备 6 类组成。

主体对客体的操作按照主体类型与客体类型的不同进行细化，以块设备为例，具体操作如表 2 所示。

表 2 块设备具体操作表

客体	操作类型	具体操作
设备类——块设备	文件操作	open：打开文件或设备； close：关闭文件或设备； read：从文件或设备读取数据； write：向文件或设备写入数据； ioctl：控制文件或设备的操作，如调整磁盘分区的大小； fsync：强制将文件系统的缓存数据写入磁盘
	设备控制	mmap：将文件或设备映射到内存中； munmap：取消文件或设备的内存映射； msync：同步内存映射区域到文件或设备； mprotect：更改内存映射区域的保护属性； fallocate：预先分配文件空间

2.3 衍生定义

操作集定义为 act（n）= {act_1，act_2，…，act_n}，代表 n 个操作组成的完成任务的动作集合。

定义判定函数 φ，如 $\varphi|\mathrm{act}(n)|>0$，代表操作集 act（$n$）包含攻击行为，$\varphi|\mathrm{act}(n)|$的值为攻击类型，例如 $\varphi|\mathrm{act}(n)|$值为 1 代表缓冲区溢出攻击。

3 操作系统行为测量

当前经典 ATT&CK（Adversarial Tactics Techniques and Common Knowledge）框架[11]与杀伤链理论[12]在安全分析中从事后追查角度能有效串连各种事件日志，可有效满足安全事件事后分析，但对于实时安全检测分析，当前的检测手段仅可实现对各种事件的“观测”，而无法实现

实时准确检测，从而影响了上述检测理论的直接应用，其主要原因是当前安全检测系统数据格式差异、从不同来源数据集进行关联分析困难、规避逃逸导致数据失真失效等问题的存在。

为解决上述问题，基于操作系统行为概念及形式化定义，将原来分离分散定义的日志事件实现以操作系统行为的统一格式定义描述，在形成统一概念的基础上将其应用于安全防护检测中，如安全防护的事前预警、事中检测与事后溯源等方面。基于操作系统行为概念，将具体操作系统行为以实时底层无感监测的方式实现数值化度量，将其定义为操作系统行为测量。

3.1 操作系统行为测量的内涵

基于操作系统行为测量定义，可以概括其相关内涵如下：

（1）本质是测量而不是观测

操作系统行为测量的本质是实现操作系统行为在统一维度下的量化度量记录，这是与原来安全观测、评测的最大区别，其有效克服了原来事件记录方式不全面、不直观的问题。

（2）核心是构建测量标准与工具

要实现标准化测量的核心是构建测量标准与测量工具，即必须确立操作系统行为测量的标准与度量工具，从而确保测量结果的准确、有效，也树立了测量结果的权威、可信。

（3）特点是测量过程实时性与透明性

对具体操作系统行为进行测量，必须强调具体测量实现与操作系统行为是同步进行的，即测量具有实时性；并且被测量对象在测量过程中不会发现测量行为，测量动作对于被测量对象是透明，即测量具有透明性。

3.2 操作系统行为测量的作用

操作系统行为测量的作用可以简述为以下几方面：

（1）在理论应用上提升 ATT&CK 框架与杀伤链理论的应用范围。目前的 ATT&CK 框架与杀伤链理论在安全攻击分析、安全事件追踪溯源上都发挥了重大作用，但实时安全检测中，往往受到安全检测系统与检测数据等因素限定，无法有效发挥作用。而操作系统行为测量结合 ATT&CK 框架与杀伤链理论，不仅能在事后追踪溯源阶段更好地实现安全事件分析定位，还能在事中检测阶段有效支撑多源异构的安全分析，从而有效扩展了 ATT&CK 框架与杀伤链理论的应用范围。

（2）在方法实现上树立安全检测的新机制。目前的安全防护与攻击系统基本处于同一层次（即操作系统内部），这种“攻防同层”部署的弊端就是安全检测可被屏蔽绕过、检测结果失真失效，而操作系统行为测量在实现上突出的透明与实时要求，改变了以前“敌暗我明”的被动局面，形成了“敌明我暗”的主动优势。

（3）在安全应用上形成安全检测数据新基准。操作系统行为理论将各种行为实现统一定义，在此基础上实现安全检测数据集，全面涵盖网络行为、文件操作、外设使用、中断调用、系统调用等多种类型，并且测量数据准确、有效，可有效支撑相关的入侵检测分析、主机防护检测、外设非法使用管控与主机安全加固等不同方面安全应用的实时分析检测；并且操作系统行为测量生成的相关数据具有准确性与权威性，还可应用于安全事件追踪溯源、事件定责与取证等方面，最终形成安全检测数据的新基准。

3.3 操作系统行为测量应具有的技术基础

要实现操作系统行为测量在技术实现上需要具备两个要求：

（1）实现部署底层化，即改变目前的在操作系统应用层部署代理或在内核中加载模块的传统方法，通过形成与网络攻击部署层次代差，最终保证测量的有效性与正确性；

（2）具有资源使用监测的全部性，改变目前安全监测采集的局限性，实现对网络、设备、系统调用、中断调用等各种资源访问的全面监测。

因此，操作系统行为测量应当独立于被测试操作系统，以“旁观者”方式实现对其进行全面的行为测量，构建形成硬软结合、多维度综合测量的实现方案。

3.4 操作系统行为测量应具备特点

相对于以前的安全监测，操作系统行为测量应当具备以下特点：

（1）可测量化：操作系统行为测量应该将具体行为通过操作系统行为理论实现其数据化或量化，最终通过测量将其转化为量化数据。

（2）可复现性：操作系统行为测量保证其测量实现的可复现，即其他测试方可以根据相同的测量方法获得相似的结果。

（3）客观性：操作系统行为测量可避免被待测方干扰，能独立客观实现对具体操作行为的测量和分析。

（4）准确性：操作系统行为测量应具有准确性，保证测量数据的准确与可信，从而有效支撑后续应用与分析。

4 操作系统行为分析模型

传统网络安全防御中，网络行为、进程行为、系统调用和设备使用等安全格式异构，导致数据分散、难以整合，不仅降低了威胁检测的性能，还难以发挥人工智能模型统一分析的效能。

在传统安全系统中，主机防火墙记录的数据内容一般为：IP 五元组（IP 源地址、IP 目标地址、协议源端口、协议目标端口及协议载荷数据）；防病毒系统的日志记录一般为：文件名、文件目录、病毒名称、检测特征等；缓冲区溢出检测的日志记录一般为：内存地址段、写入数据、异常提示、操作进程等。

APT 攻击往往会在实现中对当前的各种终端防护机制进行逃逸规避，而无法通过这些终端防护机制的检测及告警实现检测，因此往往需要从不同来源不同类型的操作日志数据进行融合分析，发现异常行为，最终实现对 APT 攻击的检测。

多维度数据关联融合问题，即从不同安全系统获取的操作数据如何实现统一的关联分析的问题。因为不同安全设备关注的重点与检测内容往往不一致，从而造成不同来源的数据缺乏统一的数据格式定义与数据内容，而要实现多维度数据关联分析，就需要从不同维度的数据集中对相关数据进行关联匹配检索查找等操作，一是需要进行大量的数据操作；二是查询检索的效率与准确性依赖于算法，都有待提升，进而影响了 APT 攻击的异常行为检测的实现。

为解决上述问题，通过操作系统行为定义统一各类行为操作，将纵向无序扩展的检测分析方法通过操作系统行为模型进行了简化（如图 2 所示），可有效解决异构数据关联融合分析、安全防护检测效能等问题。

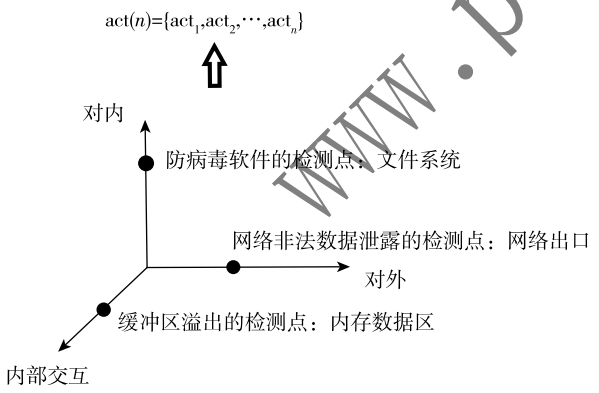

图 2　操作系统行为描述示意图

将不同维度的文件操作、内存操作、网络操作等操作行为，通过操作系统行为统一描述，归并为操作系统行为数据集，避免了原来异构数据关联分析的开销，以进程主体为主线，按照主体、对象、操作、参数与结果输出的行为组成要素，形成有效操作系统行为分析数据集合。

以操作系统行为数据集为基础，对海量操作系统行为数据集合进行有效融合分析，通过行为建模融合分析形成操作系统行为基线，将海量数据简化为少量异常数据集，进而对异常行为进行标识、判定，最终形成攻击检测规则集，如图 3 所示。

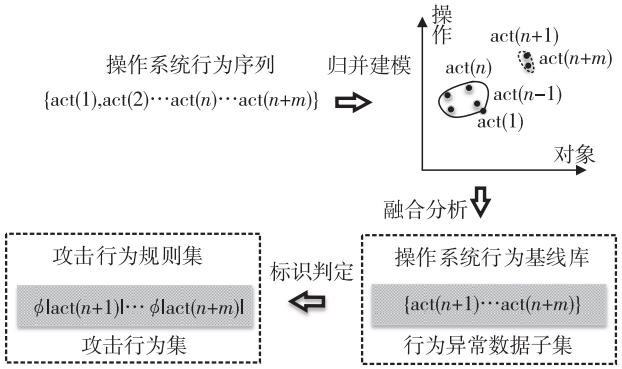

图 3　操作系统行为分析模型示意图

5　操作系统行为理论应用示例

5.1　缓冲区溢出攻击分析

缓冲区溢出攻击[13]的传统定义为：通过向某一程序缓冲区写入超出其长度的内容，造成缓冲区溢出，从而破坏程序的堆栈，使程序转而执行其他指令，以达到攻击的目的。

基于操作系统行为理论，重新进行缓冲区溢出攻击的形式化定义如下：

缓冲区溢出攻击为：$\varphi|\mathrm{act}(n)|=\varphi|(p_{\mathrm{id}},o_n,a_n,d_n,r_n)|=01$，且 $(p_{\mathrm{id}},o_n,a_n,d_n,r_n)=(p_{\mathrm{xxx}},o_{\mathrm{men}},\mathrm{mem}_{\mathrm{write}},d_{\mathrm{write}}\rightarrow r_x)$ 执行成功。

此时，主体属性 $P_{\mathrm{type}}|p_{id}|=1$，代表为进程；地址空间：$\mathrm{Memzone}|p_{\mathrm{id}}|=\{\mathrm{Low},A;\ \mathrm{High},A+L\}$。

d_{write} 包含参数 $d_1=D_{\mathrm{writedata}}$ 为内存写入起始地址；$d_2=m$ 为写入数据字段长度；$d_3=\mathrm{Data}_{\mathrm{writedata}}$ 为写入数据字段。

缓冲区溢出相关限定条件为：$A<D_{\mathrm{writedata}}\leqslant A+L$ 且 $D_{\mathrm{writedata}}+m>A+L$。

通过对比上述缓冲区溢出攻击的定义，可以发现基于操作系统行为理论的概念定义更加准确，其特点在于：

（1）实现对攻击行为的形式化定义描述，将原来基于概念的描述方式升级为具体的形式化定义，具有更高的科学性；

（2）在科学定义的基础上实现对攻击的数值量化，进而有效支撑基于操作系统行为的攻击分析检测。

5.2　终端数据泄露攻击分析

终端数据泄露[14]是指恶意程序非授权访问敏感数据，并通过网络或外设隐匿向外传输。目前的终端数据防泄露手段往往是通过在网络或外设出口处实施基于特征匹配的数据审查，防止敏感数据外传。现有数据防泄露的

着力点在于发现并阻止敏感数据的外传，从而确保敏感数据的保密性。其优点在于能快速部署阻断敏感数据非法外传，但其基于特殊匹配的检测方式，可被攻击方通过传输加密等方式规避。

针对传统数据防泄露系统的不足，本文设计了基于操作系统行为测量的数据防泄露机制。其特点在于通过操作系统行为方法来分析数据泄露的整个流程。

基于操作系统行为理论，重新进行终端敏感数据泄露攻击的形式化定义，如下：

终端敏感数据泄露攻击为：$\varphi|\mathrm{act}(n)|=\varphi|(p_{\mathrm{id}}, o_n, a_n, d_n, r_n)|=09$（09 代表数据泄露攻击），且 $(p_{\mathrm{id}}, o_n, a_n, d_n, r_n)=(p_{\mathrm{xxx}}, o_{\mathrm{file}}, f_{\mathrm{read}}, d_{\mathrm{read}}\rightarrow r_{\mathrm{read}})$ 非授权文件读操作执行成功，输出结果为 r_{read}（非授权读取的文件）并且 $(p_{\mathrm{xxx}}, o_{\mathrm{net}}, n_{\mathrm{send}}, r_{\mathrm{read}}\rightarrow r_{\mathrm{sead}})$ 非法读取的文件 r_{read}网络发送执行成功。

对终端敏感数据泄露进行操作系统行为形式化定义分析，可以发现数据泄露的过程包括两个阶段：（1）非授权文件读操作，攻击方可利用操作系统或应用程序漏洞绕过文件访问控制机制，读取超过其授权的文件；（2）对外隐匿传输，将获取的敏感数据通过网络或其他隐匿通道向外传输。

基于上述分析，要防止终端敏感数据泄露必须针对这两个非法操作同时进行防护，既要防止终端内部文件不会被非授权读取，也要阻止敏感数据的外传。因此，在传统终端敏感数据防泄露系统的功能基础上，还需要加强文件系统的访问控制与权限管理，结合大数据分析技术[15]，并有效修补系统漏洞，才能治标治本，从源头与渠道两个方面防止终端敏感数据泄露。

6 结论

本文研究了以行为概念为基础的操作系统行为理论，设计了操作系统行为分析模型，定义了操作系统行为主体、客体、操作与结果输出的概念，将研究目标聚焦于操作系统行为监测，将安全事件通过操作系统行为定义，形成了统一行为数据分析基础数据，并以其为基础进行操作系统异常行为融合分析，进而构建操作系统行为标准基线，有效判定各种已知与未知攻击行为。

操作系统行为理论模型改变了原来以攻击结果为目标抓手的防护思路，其特点在于：

（1）在理论上具有科学性。操作系统行为形式化定义方法在理论上突出两个转变：一是实现了从问题应对处置到溯源剖析的转变；二是从表象解除至致因控制的转变。

（2）在分析技术上具有先进性。将纵向无序扩展的检测分析方法，通过操作系统行为模型进行了简化；有效解决异构数据关联融合分析、安全防护检测效能等问题。

为扭转攻防同层导致“测不准”的弊端，下一步的研究方向为设计实现操作系统行为的透明测量，确保操作行为测量的准确性、有效性与正确性。

参考文献

[1] 褚龙，伍荣，龙飞宇. 端点检测与响应技术及其发展趋势 [J]. 通信技术，2017，50（7）：1493－1498.

[2] 王永非. 基于行为分析的检测 APT 攻击方法的研究与实现 [D]. 北京：北京邮电大学，2019.

[3] 陈卫平. 高级持续性威胁检测与分析技术初探 [J]. 现代电视技术，2018（11）：135－137.

[4] 宋首友. 智能终端控制及隐私保护研究 [D]. 北京：北京邮电大学，2015.

[5] 王轶骏，代传磊. Linux 终端检测响应系统的文件防护绕过技术研究 [J]. 通信技术，2024，57（9）：934－941.

[6] 杜彦辉. 信息安全技术教程 [M]. 北京：清华大学出版社，2013.

[7] 王春光. 虚拟机操作系统行为监控技术的研究与实现 [D]. 长沙：国防科学技术大学，2009.

[8] 樊燚，郭义伟，胡涛，等. 基于系统调用的主机异常检测研究综述 [J]. 信息工程大学学报，2024，25（1）：100－109.

[9] 张凯. 面向操作系统内核的深度学习方法研究 [D]. 长沙：湖南大学，2023.

[10] 王帅，汪来富，金华敏，等. 网络安全分析中的大数据技术应用 [J]. 电信科学，2015，31（7）：145－150.

[11] 朱子枫. 基于 ATT&CK 技战术的网络攻击效果评估指标体系构建及计算研究 [D]. 广州：广州大学，2024.

[12] 刘文彦，霍树民，陈扬，等. 网络攻击链模型分析及研究 [J]. 通信学报，2018，39（S2）：88－94.

[13] 滕翠，梁川. 基于虚拟现实技术的网络渗透仿真训练系统设计 [J]. 自动化与仪器仪表，2016（2）：197－200.

[14] 李志勇. 一种基于终端安全技术的数据防泄露系统的设计与实现 [D]. 长沙：湖南大学，2011.

[15] 刘冬兰，刘新，张昊，等. 基于大数据业务场景的数据安全分析及防泄露技术研究 [J]. 山东电力技术，2020，47（9）：7－13.

（收稿日期：2024－10－16）

作者简介：

祝林（1977－），男，博士，高级工程师，主要研究方向：网络安全、操作系统安全。

邬江（1978－），男，硕士，高级工程师，主要研究方向：网络安全、数据安全。

刘克斌（1976－），男，硕士，工程师，主要研究方向：网络安全、大数据。

版权声明

凡《网络安全与数据治理》录用的文章，如作者没有关于汇编权、翻译权、印刷权及电子版的复制权、信息网络传播权与发行权等版权的特殊声明，即视作该文章署名作者同意将该文章的汇编权、翻译权、印刷权及电子版的复制权、信息网络传播权与发行权授予本刊，本刊有权授权本刊合作数据库、合作媒体等合作伙伴使用。同时，本刊支付的稿酬已包含上述使用的费用，特此声明。

《网络安全与数据治理》编辑部