基于系统调用的入侵检测研究进展

吴 瀛 江建慧 张 蕊
(同济大学计算机科学与技术系 上海 200092)

摘 要 基于系统调用的入侵检测是当前信息安全领域的研究热点之一。全面分析了已有的基于系统调用的入侵检测的理论与技术,总结了近年来的研究进展,并对其发展趋势进行了展望。随着基于Tide的商用系统SanAPT的推出,需要进一步研究的将是提高检测性能,降低误报率,解决与实用化相关的多平台、轻量化、分布化等方面的问题。

关键词 入侵检测,系统调用,多平台,轻量化,分布化
中图法分类号 TP393 **文献标识码** A

System Calls Based Intrusion Detection: A Survey

WU Ying JIANG Jian-hui ZHANG Rui
(Department of Computer Science and Technology, Tongji University, Shanghai 200092, China)

Abstract System call based intrusion detection is currently a hot subject of research all over the world. The existing system call based intrusion detection techniques and theories with their respective challenges and research trends were discussed comprehensively, especially those(that are) newly developed. We hold that with the advent of the Tide-based commercial intrusion detection system(IDS) SanAPT, how to improve detection performance, to decrease error alarm rate and to solve issues on multiplatform, lightweight, and distribution related to practicality of the IDSs will be hot topics in this field.

Keywords Intrusion detection, System call, Multiplatform, Lightweight, Distribution

1996年,Sundaram认为系统调用序列用于误用入侵检测时,可以克服击键序列所存在的某些缺点[1]。同年,Forrest等指出,特权进程的系统调用局部短序列具备明显的一致性,可以区分不同的特权进程、敏感于进程的异常行为,并首次提出基于系统调用的异常入侵检测技术[2]。

1 基于系统调用的入侵检测的主要技术

基于系统调用的异常入侵检测分两个阶段:第一阶段,扫描正常行为轨迹,根据系统调用序列构建正常行为模式特征库;第二阶段,扫描可能含有异常行为的新轨迹,查找正常行为模式特征库中未出现的模式[2](以检测是否受到入侵)。迄今为止,基于系统调用的入侵检测主要有序列枚举法、统计学方法、基于机器学习的方法、基于数据挖掘的方法以及基于有限状态机的方法等。

1.1 序列枚举法

序列枚举法[2-4]通过滑窗技术枚举正常进程轨迹中的定长系统调用短序列的方法来建立正常特征库:被监控进程出现特征库以外的短序列称为一次失配,失配数量大于阈值则标记为入侵行为。

目前,序列枚举法主要有两种特征库。Tide特征库记录各短序列首个系统调用后续各位置的许可系统调用集[2];Stide[3]和W检测[4]的特征库则由完整的定长系统调用短序列组成。Tide和Stide的建库和检测过程均基于进程发出的全部系统调用,W检测则仅仅关注具备"写"性质的系统调用子集。

检测时,Tide采用前向匹配对(lookahead pair)[5]技术逐个检测序列内首个系统调用与第1至第k个位置的系统调用之间的K个匹配关系,不考虑这k个系统调用内部之间完整的时间关系;Stide和W检测则将整个系统调用短序列看作一个完整的时序事件。从信息容量看,Stide技术检测的信息量比Tide更丰富,因而准确性更高,并长期受到关注[4,6]。W检测[4]的贡献在于缩小了特征数据库的规模,降低了存储和计算代价。但W检测仅仅考虑具备"写"性质的系统调用子集,一旦入侵行为绕过W子集,就有可能导致漏检现象。

1.2 统计学方法

统计学入侵检测方法采用统计量作为轮廓描述系统调用序列的行为特征。该类检测系统通常维护两个轮廓:已存储的正常行为轮廓和被监控进程的当前行为轮廓,并采用当前轮廓与正常行为轮廓之间的差值是否超过阈值作为判断入侵行为的依据。

T-Stide统计各短序列在训练数据集中的出现频率,频率小于0.001%的短序列出现在被监控的系统调用轨迹被视为异常[5];ScanAID根据正常系统调用序列中所有唯一性的、长为w的系统调用短序列(w-gram)的出现频率$P(w_i)$,计算各

到稿日期:2010-03-09 返修日期:2010-05-18 本文受863国家重点基金项目(2007AA01Z142)资助。
吴 瀛(1970—),男,博士生,讲师,主要研究方向为信息安全、入侵检测等,E-mail:woo_ian@ustc.edu;江建慧(1964—),男,教授,博士生导师,主要研究方向为可信计算、信息安全、软件可靠性工程等;张 蕊(1980—),女,博士,主要研究方向为可信计算、应用安全等。

短序列最后一个系统调用的异常指标(同一系统调用存在多个异常指标时取最大值),并将被监控进程完整轨迹的各系统调用异常指标值之和作为统计量,以判别异常[7]。AHDAD(均值海明距离入侵检测)则采用正常行为进程和被监控进程的系统调用短序列集之间基于U统计量的均值海明距离作为入侵判别统计量[8]。

该类技术无需入侵行为特征的先验知识。缺点是易受到入侵者的反向训练而出现漏检现象、某些进程难以满足该方法所基于的准稳态假设。此外,阈值确定也是一个困难问题。

完整的进程运行轨迹的系统调用(序列)的统计学特性呈现出稳定性[3],并表现为时间的函数。仅当系统调用(序列)样本足够大时,统计量才稳定。正常行为系统调用短序列库的统计量反映的是完整系统调用轨迹的稳定的统计学特性,要实现准确的入侵检测,被监控进程的轨迹也必须是完整的。因而,该技术很难实现实时检测。

1.3 机器学习方法

1.3.1 K近邻分类器法

基于K近邻分类器的系统调用入侵检测技术[9-11]依据于文本分类和入侵检测的相似性(见表1)。Liao[9]采用进程中各系统调用出现的频率将单个进程的完整系统调用序列转换为向量空间中的M维向量(M为不同的系统调用的个数),被测进程的异常指标是轨迹向量与其最邻近的K个正常进程轨迹向量之间的平均余弦相似度。

表1 kNN分类器用于文本分类与入侵检测的相似点

术语	文本分类	入侵检测
N	文本总数量	进程运行轨迹总数
M	不同单词总数量	不同系统调用总数
n_i	第i个单词出现次数	第i个系统调用的出现次数
f_{ij}	文本j中第I个单词的出现频率	第j个轨迹中第I个系统调用出现频率
D_j	第j个训练文本	第j个系统调用轨迹
X	目标检测文本	目标检测轨迹

后续研究主要集中于相似度量。平均余弦相似度仅考虑系统调用频率[9];与平均余弦相似度相比,二元加权余弦相似度(BWC)[10]还考虑了不同进程间相同的系统调用及其频率。核基函数(KBF)度量、平滑核基函数(SKBF)度量、二元加权径基函数(BWGRB)度量以及平滑二元加权径基函数(SWGBRB)度量等[11]采用了核方法的思想。核函数处理高维特征空间的能力,较好地改善了此类检测器的性能,但其工作原理决定了该类技术无法实现真正的实时检测。

1.3.2 基于生物免疫学的学习方法

进程的"自我"概念[2]首次将入侵检测转化为区分进程的"自我"和"非我"的问题。Forrest[12]受T细胞成熟过程中阴性选择的启发,构造了"抗体(检测子)"生成算法并引入了部分匹配思想。但该算法生成的候选检测子大部分被抛弃,且时间复杂度与自我集大小呈指数关系。

基于生物免疫学的入侵检测系统最常用的模型是自我-非我模型[13],关键是"自我"的表达、检测子(抗体)的生成与演化、空洞避免和匹配规则的设计与优化。目前,匹配规则主要有r连续位、r-chunk、前向对以及n-gram等4种。这些匹配规则各有优缺点。例如,前向匹配对技术容易导致漏报[14];r-chunk比r连续位检测粒度更细,但代价相对较高等。检测子生成主要有随机生成算法[12]、线性时间生成算法[15]和贪心生成算法[15]。线性时间与贪心生成算法分别从时间复杂度和非我域覆盖度等方面改进了随机生成算法。为减少"空洞",增大覆盖率,有人提出了置换掩码技术[16]。

近年来,免疫学领域又提出了一种称为危险模型的新免疫学模型[17]。该模型同样引起了人工免疫学入侵检测领域的关注[18,19],但这些工作有待进一步深入研究。

免疫学检测技术具备良好的分布性、高效性、无通信协作能力以及自我集与检测器集的双向保护功能,不失为最有发展前途的技术之一。但该领域还存在大量有待进一步研究的问题,例如洞避免、匹配规则的优化、检测器的生成与动态演化等。

1.3.3 基于马尔可夫模型的学习方法

计算机发出的当前系统调用序列只与前一时刻发出的系统调用序列直接相关,而和前一时刻以前发出的系统调用序列不相关[20]。因此,可以采用马尔可夫模型来分析进程的系统调用。

通过选择合适的参数,隐马尔可夫模型可以理想地处理时变随机过程。较早基于马尔可夫模型的系统调用IDS采用了全连接隐马尔可夫模型[5,21],状态数与进程所发出的系统调用的种数大致相等,转换概率矩阵使用Baum-Welch算法[22]训练。该方法检测准确性较好,但计算代价较大[5]。除非解决了计算复杂性等问题,该类模型才能很好地用于入侵检测[23]。

S. Cho等基于入侵领域知识,仅考虑特权转换流来建立隐马尔可夫链,在不降低检测性能的同时,显著地提高了训练效率[24];Tokhtabayev等认为非平稳马尔可夫链可以更好地描述应用或服务的行为模式,并根据异常传播模式与网络主机连接模式的一致性判断恶意行为的可信性,极大地减少了误报率,提高了检测准确性。该领域的其它大量研究工作如表2所列。

表2 基于马尔可夫链的学习方法

作者	特点
X. D. Hoang等[26]	完整系统调用序列分成多个子序列,每个子序列训练一个子模型。最后,将各子模型合并到最终的HMM模型中。
W. Wang等[27]	采用系统调用短序列而不是系统调用作为可观察输出量;仅考虑输出可观察量的转换概率;利用失配百分比等统计量。
Ye, D.等[28]、谭小彬等[30]	仅关注HMM模型的第一个基本问题,并基于相对概率(relative probability)构建分类器[32],判断是否出现异常行为。
S. Han等[29]	按规则将基于系统调用的HMM模型、统计学模型,以及BLP模型整合成一个多度量检测系统。HMM监控系统调用序列;统计学模型监控系统资源的使用以及发出的系统调用数量;BLP模型监控对文件的存取。
尹清波等[20]	采用线性预测技术从系统调用序列中提取特征向量建立正常特征库,据此建立马尔可夫模型,并根据马尔可夫模型输出的状态序列概率确定是否出现了入侵行为。
尹清波等[31]	将长为K的系统调用短序列作为特征向量建立正常特征库,以特征向量作为状态构建动态马尔可夫模型。用有限的数据集实现更精确的模型训练。
张响亮等[32]	将系统调用短序列作为HMM的可观察输出量,根据系统调用短序列的输出概率是否大于阈值判断是否出现异常行为。
闫巧等[33]	用正常系统调用轨迹训练HMM,再通过系统调用轨迹和已训练好的HMM获得最佳状态转移序列。采用滑窗技术,构建最佳状态转移短序列正常轮廓库。被测进程的最佳状态转移短序列不在库中,则标记为失配;失配超过预定阈值,则报警。

基于马尔可夫模型的入侵检测方法的检测准确性优于其它常见方法,缺点是对噪音数据较为敏感、训练时间过长。目前的大部分工作是从马尔可夫链的构造过程或者马尔可夫链的状态及可观察输出量等方面着手改进马尔可夫链的存储及

计算代价。实际上，缩短马尔可夫模型训练时间最有效的方法可能是改进其参数估计算法和评估算法。

1.3.4 基于神经网络的学习方法

Ghosh 等[34]、Endler 等[35]应用人工神经网络学习系统程序行为和系统调用序列，并实现入侵检测。Ghosh 采用反向传播神经网络通过正常数据集和异常数据集对多层前向神经网络进行训练，训练过程以网络输出的总误差不再增长为结束条件，采用漏桶算法弱化偶然性异常行为并强化猝发性异常行为对入侵检测阈值的贡献。但是，反向神经网络不能很好地处理 BSM 特征大规模结构，Ghosh 等进一步采用 Elman 网络来实现入侵检测。Elman 网络的上下文节点具备记忆功能，可以识别循环特征，其检测性能更加优异[34]。Endler 采用神经网络分析的是用户会话所发出的系统调用序列，Ghosh 则是分析单个进程的系统调用序列。该领域的主要后续研究参见 Rapaka 等[36]、Zhang 等[37]和李千目等[38]的工作。

通过学习，神经网络可以根据不完全、复杂、非确定性的数据集获得输入和输出之间的非线性映射；配合适当的实现技术，可以兼具误用和异常入侵检测技术的优点。但计算复杂性随神经元的个数增长而快速增长，因此寻找合适的网络（如 Elman 循环网络[34]、径基函数网络[36]）、确定合理的网络规模、提高检测准确性、降低计算复杂性以及与其它技术组合实现 IDS（见文献[37,39]）等是其主要努力方向。

1.3.5 基于支持向量机的学习方法

支持向量机（Support Vector Machine，SVM）[40]用于系统调用入侵检测的关键是选择或构建核函数。核函数必须是正定的（Positive Definite）、满足 Mercer 条件、确保核是给定特征空间内真正的点积。常见的核有多项式核、径基核及 Sigmod 核。Tian 等[41]设计了一组序列核以实现基于 SVM 的系统调用异常检测。其中，公共子串核容许子序列之间存在间隙，为较长子串赋予较大权值，并对所有尽可能长的公共子串进行计数。序列核均考虑系统调用序列的时间顺序信息，比常见核函数更适合系统调用异常检测。

也有一些研究工作采用 SVM 辅助其它分类器来实现入侵检测[39]。该领域的主要研究热点是构建核函数、解决过学习（Over fitting）及大数据集计算复杂性[42]等问题。

基于机器学习的系统调用异常检测技术还采用了诸如贝叶斯网络、基于动态贝叶斯网络的入侵意图预测[43]等方法，限于篇幅，不再详述。

1.4 数据挖掘方法

数据挖掘[44]用于入侵检测的基本思想是根据海量数据综合利用各种挖掘方法建立模型，自动、高效地建立智能 IDS。数据挖掘方法通常输出以决策树或规则表示的分类器，并用分类器将审计数据划分为正常或异常类别来实现入侵检测。

Lee 等[45,46]采用 RIPPER 算法进行挖掘，主要不同点在于判断异常的分类规则。前者输出一系列 if-then 规则集。例如，若短序列的第 2 个位置为 VTIMES，第 7 个位置为 VTRACE，则被检测短序列正常；第 2 个模型则是由短序列前 $m-1$ 个系统调用对第 m 个系统调用进行预测的规则集构成。例如，若短序列的第 3 个属性为 LSTAT，第 4 个属性为 WRITE，则第 7 个系统调用为 START。这两类规则均采用系统调用中的控制流信息实现入侵检测。基于上述研究，Lee 等[47]还提出了一种基于数据挖掘的形式化入侵检测模型。

除了控制流信息外，系统调用的参数还形成丰富的数据流信息。Li 等[48]采用控制流分析，提取进程轨迹中的变长系统调用短序列模式；借助关系挖掘技术，从短序列模式中挖掘出 3 种分类规则，分别监控单个模式系统调用短序列内的系统调用参数与返回地址的关系、重复出现的同一模式系统调用短序列在不同轮次中参数之间的关系以及不同模式系统调用短序列的参数之间的关系。这些规则同时检测了程序运行过程中的数据流和控制流信息，具有良好的检测性能，且系统开销较小。

基于数据挖掘的异常检测技术的检测性能与训练数据的完备性、从系统调用提取的规则属性、规则属性的数量以及规则的有效性等均有密切关系。Li 等[48]为规则属性的提取与处理提供了一种新思路，该领域在研究更加优秀的分类技术、选择合适的系统调用[49]、提取合理的规则属性并确定其数量等方面可能会引起更多的后续工作。

1.5 其它基于系统调用的入侵检测技术

1.5.1 基于审计事件向量的入侵检测

基于审计事件向量的入侵检测模型（AUDIDS）[50]通过实时收集审计事件来实现入侵检测。审计事件是系统中所有与安全相关的活动。审计事件一部分是在关键系统调用的基础上扩充而成，另一部分则是在特权进程或关键程序的基础上建立而成。与无参数系统调用相比，审计事件语义更丰富，检测性能更好，且采用后向匹配算法，效率更高。但是，该方法的检测准确性严重依赖于正常库的完备性，另外需要修改操作系统内核也是该技术的另一个不足。

1.5.2 基于有限自动机的入侵检测

Kosoresow 等[51]较早采用确定型有限状态机（DFA）来分析进程的系统调用序列。该工作根据正常系统调用序列首先生成一系列的宏（变长系统调用模式序列），描述进程主体频繁出现的系统调用所组成的串和长为 2～6 个系统调用组成的公共模式串。然后，将正常系统调用轨迹表示为宏序列。为缩短系统调用轨迹的序列长度，采用 kleene 闭包处理连续出现的紧邻宏，得到了系统调用轨迹的超集。最后，根据正常系统调用轨迹的宏序列，构建 DFA 描述可能的正常系统调用轨迹，如图 1[51]所示。

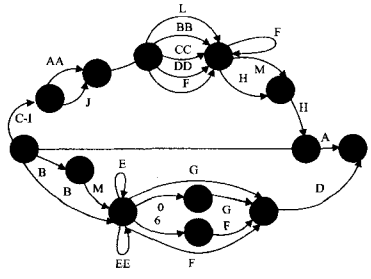

图 1 DFA 表示的进程正常系统调用轨迹

文献[51]揭示了进程正常行为中的正则结构（Regular Structure），但存在 DFA 状态难确定、自动机规模与宏构建代价过大、无法自动构建等问题。

Sekar 等[52]从程序可执行文件中提取出系统调用的调用点（程序计数器）的程序状态信息，解决了 DFA 的全自动构建和规模过大等问题。Wagner 等[53]基于程序源代码静态分析技术，为应用程序的期望行为提出了对后续研究影响较大的

调用图(Call graph)模型和抽象栈模型。

该领域的主要工作是解决自动机的时间空间代价和不确定性等问题。主要是采用静态分析或动态分析技术，获取进程运行状态的相关信息(手段主要有位置相关、上下文相关、内存块相关)，减少不可达路径；通过优化技术(主要有合并单后续状态、合并终态、合并等价转换符等)，降低状态机检测模型的运行开销。由于动态分析方式和静态分析方式所建立的模型分别为程序正常行为的子集和超集[54]，近年有人提出混合使用静态和动态分析技术以更精确地描述程序的正常行为(见表3)。

表3 基于有限自动机的系统调用异常入侵检测技术

模型	自动机类型	模型简述	备注
2001 Compact FSA[52]	有限状态机	借助系统调用点的程序状态(计数器指针信息)区分自动机的不同状态；可以跟踪系统调用之间的或长或短的时间顺序信息，可以跟踪程序的结构信息，例如分支、跳转、汇聚等，并给不同异常赋予不同权重。	动态构建；对系统调用序列的长度无限制；训练过程快；检测准确性高；误报率更低；时间与空间开销更小；缺乏对动态链接库的处理。
2001 抽象栈模型[53]	非确定型 PDA	源代码静态分析技术；将系统调用和程序计数器关联起来，实现确定型自动机。	监测准确的函数调用与返回信息；对动态链接库处理过于简单，可能导致漏检；可以检测借助不可达路径实现的入侵；模型开销极大。
2003 VtPath 模型[55]	下推自动机	结合调用栈历史信息和程序计数器值，构建虚拟栈表，借助虚拟栈表计算当前系统调用与上一个系统调用之间的不定虚拟路径(adhoc virtual path)，并验证该路径的合法性。	动态训练过程中建立模型，对调用栈中的返回地址进行监控，较好地处理了动态链接库中的函数调用及这些函数发出的系统调用。
2004 VPStatic 模型[56]	全确定型 PDA	采用观察(observational)技术；从二进制代码中提取出地址信息，构建虚拟栈表，实现 PDA 模型的确定化。	静态分析二进制代码来构建，为 VtPath 模型的静态构建版本，无需更改二进制可执行代码；具备异常恢复功能。
2004 Dyck 模型[57]	栈确定型 PDA	采用内联技术构建整个进程的自动机；探讨了静态可确定参数恢复技术、分支分析技术、二进制代码插装技术、空调用抑制技术、进程内数据流分析技术、空系统调用插入技术等对检测性能和效率的影响。	静态二进制代码分析构建的上下文相关模型；消除了栈转换过程的非确定性，降低了运行开销；准确性比上下文无关模型提高一个数量级。
2005 HPDA 模型[54]	栈确定型 PDA	静态分析二进制代码，根据可执行文件的控制流图构建基本模型；动态学习程序运行过程的调用栈信息，以获取静态代码缺乏的或者动态链接库等中的控制流信息。	结合了动态模型和静态模型的优点。该模型与动态或静态模型相比，能更加精确地描述程序的正常行为；检测性能更优于 wagner 等的模型。
2007 EMPDA 模型[58]	FSA(核心模型)	按系统调用的重要性不同，分别建立核心模型和辅助模型；采用行为-响应对之间的逻辑关系，建立约束模型以检测程序安全运行必须满足的约束关系。	进一步扩展了 HPDA 模型；核心模型保证准确性，辅助模型提高泛化能力。模型细分提高了覆盖速度；检测准确性优于 HPDA，效率更高。
2009 HFA 模型[59]	下推自动机	提出了动态绑定思想，对静态分析过程中建立的局部确定有限自动机直到程序运行时刻才进行绑定操作，以建立完整的 HFA 模型，并在运行时刻对非标准跳转流进行修正处理。	解决了静态绑定导入的不确定性；解决了静态分析不能解决的间接函数调用和跳转问题，比上下文相关模型更接近确定型 PDA。检测精确性与效率比 Dyck 等模型都优秀。

此外，Gopalakrishna 等[60]也提出了自动机内联技术，着重探讨了各种自动机优化问题并宣称其成果同样适用于基于系统调用的入侵检测。

基于自动机的检测技术的优点主要有误报率低，以静态分析方式构建良好的下推自动机的误报率理论上为零；实现手段成熟，无论是构建技术还是自动机语言等方面，自动机均拥有丰富的理论研究成果与实践经验可供借鉴。目前来看，其挑战仍在于减少不确定性以及实现系统开销与检测性能之间的平衡。

2 基于系统调用的入侵检测理论研究进展

基于序列串更改检测，Forrest 等[12]数学地证明了检测用串的数量可以根据目标检测率进行调节，两个任意串匹配的概率以及漏检概率不变时，检测用串的数量与需保护的本我串数量无关，很难通过本我串反向训练检测器等一系列结论并开创了系统调用异常检测这一研究领域。

2.1 阳性和阴性检测技术形式化理论框架

为了分析与评估基于部分匹配规则的各类检测技术，阳性和阴性检测技术形式化理论框架[61]按照正常库的表达形式和匹配连续性，将系统调用异常检测技术分为阳性连续、阳性非连续、阴性连续和阴性非连续等4类。基于二进制序列串检测，证明了 r-连续位和 r-chunk 匹配规则下，阴性非连续和阳性连续检测方案的检测能力是相同的；转换掩码技术增强了 r-连续位匹配规则的检测能力，使其非常好地包含了海明距离的识别能力；即使采用转换掩码技术，r-连续位匹配规则也不能识别某些语言。并且，该理论首次在 r-chunk 匹配规则下，对阴性非连续和阳性连续检测方案在不同情况达到最高检测能力所需检测子的数量进行了探讨。

2.2 Stide 及类 Stide 入侵检测技术形式化理论框架

Stide 及类 Stide 入侵检测技术的形式化理论框架[6]源于“魔数 6”问题[62,63]。

Lee 等[62]认为条件熵可以量度训练数据的规则性，并据此得出针对 sendmail 数据集 Stide 检测器窗口大小的最佳值为 6 或 7；Tan 等[63]则认为“魔数 6”由最小外来序列的长度决定。其分析表明 Sendmail 数据集中 dec-1 的系统调用轨迹的最小外来序列的长度为 6，从而认为对于 NMU 数据集，检测器窗口必须大于等于 6。有意思的是，该研究工作还用实验方法证明了条件熵不影响 Stide 的检测性能，其更不能作为 Stide 检测器窗口大小的确定量度。

Li 等[6]定义了外来序列、本我序列、最小外来序列、最长本我序列及上述序列所构成的集合等概念和该集合上的运算规则。借助理论分析，得出一系列等价条件，用以判断定长窗口的 Stide 检测器的完备性、有效性以及有效 Stide 检测器的存在性等；解释了伪装攻击和入侵信息隐藏绕过入侵检测器的工作原理、T-Stide 性能不佳的原因、局部帧数(LFC)的意义等。对于 Stide 及类 Stide 检测器的优化设计，该形式化理论还分析了训练数据集完备性与检测性能之间的关系，给出了训练数据集的完备性评估方法以及决定检测器检测性能的训练数据集关键区域的识别和裁定方法，探讨了系统调用参数对入侵检测性能的作用与影响等困扰人们的许多问题。

阳性和阴性检测技术形式化理论框架过于关注特定的匹配规则，普遍性意义受到一定限制且没有考虑系统调用序列

中的循环结构以及系统调用的参数等问题。程序中的循环、跳转以及用户需完成任务的统计学特性，决定了系统调用序列不是随机性的，且系统调用的频度也相当程度地反映了程序的正常行为。文献[10]中的最小外来序列、最长本我序列等在一定程度上体现了系统调用序列中的循环结构，但对系统调用参数的分析明显不足。该理论另一个明显的缺陷是没有考虑系统调用频度或频率的作用。

系统调用异常入侵检测的理论研究总体上进展缓慢，且分散于大量文献，系统性成果很少。目前的理论存在诸多缺陷，但仍在缓慢地加以完善。例如，从信息的阴性表达(Negative representation)集获得原始的阳性表达集是一个NP困难问题[64]，实际上进一步证明了文献[12]中的很难反向训练检测器这一结论。

3 基于系统调用的入侵检测技术发展趋势

3.1 代表性的技术

从入侵及入侵检测的机理来看，人工免疫学最有希望提供合理的入侵检测模型；从检测效率与泛化能力来看，支持向量机具备完善的数学理论基础；从进程行为表达能力来看，自动机及自动机语言最强，且拥有丰富的理论与实践成果可供借鉴。因此，这是3个最具代表性的方法学发展方向。

一些基础性的工作仍需要做深入的研究，比如系统调用序列到底提供了哪些信息？这些信息对入侵检测性能的贡献有多大？它们是怎样相互作用，并体现进程的行为特征的？例如有人认为，近年基于系统调用参数及系统调用信息流的入侵检测技术研究[48,65]、有必要考虑系统调用短序列模式出现的次数[66]等；针对系统调用频度信息对检测性能的贡献，作者也做了一些初步探讨[14]。

3.2 多平台

目前，基于系统调用的入侵检测技术研究主要集中在UNIX，Linux，SUN-OS等操作系统平台。随着SanAPT[67]的推出，基于其它操作系统平台的IDS研究将成为该领域的热点之一。例如，2008年Mazeroff等[68]和朱莺嘤等[69]在Windows平台上对基于系统调用的入侵检测技术开展了研究。

3.3 轻量化

合理的计算和存储代价一直是基于系统调用的入侵检测技术的一个研究热点。基于系统调用的入侵检测技术总体上属于异常入侵检测技术。与误用入侵检测技术相比，只有解决了该技术固有的计算复杂性和存储复杂性等问题，才能实现广泛的实用化与商业化。

3.4 分布化

随着网络系统的复杂化、大型化及入侵行为所具有的协作性，IDS的体系结构由集中式向分布式发展[70]。基于生物免疫学和系统调用的入侵检测技术由于具有检测性能与检测代价的可调节性、无通信协作检测能力等特点，因此极具分布式检测潜力。但也存在一些技术难题，例如基于生物免疫学的检测系统分散部署于多台主机上时，将面临抗体分配、联合报警等问题；如何利用并在本领域实现人工免疫学中的基因机制及其它当前被忽视了的其它机制[71]。

3.5 安全技术综合集成与标准化

基于系统调用的入侵检测技术的实用化与商业化进展已经初见端倪，因此需要研究安全技术综合集成与标准化[70]。此外，有学者还提出设计轻量级IDS组件，并将其整合至操作系统之中的构想。

3.6 基于系统调用的入侵检测形式化理论框架研究

入侵检测形式化理论框架可以用来对入侵检测技术进行描述、分析和评估。目前的理论成果明显滞后于技术发展进程，且无法实现量化分析与评估。因此，基于系统调用的入侵检测形式化理论研究有可能得到更多的关注。

结束语 本文力求全面、详尽地总结近年来国内外基于系统调用的入侵检测研究成果。随着基于系统调用入侵检测技术商业化进程的加速，进一步提高检测性能，降低误报率，解决与实用化相关的多平台、轻量化、安全技术综合集成与标准化等问题，将成为该领域近期主要的研究方向。

参 考 文 献

[1] Sundaram A. An Introduction to Intrusion Detection [J]. Crossroads, 1996, 2(4): 3-7

[2] Forrest S, Hofmeyr S A, Somayaji A. A Sense of Self for Unix Processes [C]// McHugh J, ed. Proc. of 1996 IEEE Symposium on Security and Privacy. Oakland, CA, USA: IEEE Computer Society, 1996: 120-128

[3] Hofmeyr S A, Forrest S, Somayaji A. Intrusion Detection Using Sequences of System Calls[J]. Journal of Computer Security, 1998, 6: 151-180

[4] 张相锋，孙玉芳，赵庆松. 基于系统调用子集的入侵检测[J]. 电子学报，2004，32(8)：1338-13341

[5] Warrender C, Forrest S, Pearlmutter B. Detecting Intrusions Using System Calls: Alternative Data Model[C]// Proc. of 1999 IEEE Symp. on Security and Privacy. Los Alamitos, CA, USA: IEEE Computer Society, 1999: 133-145

[6] Li Z, Das A. Analyzing and evaluating dynamics in stide performance for intrusion detection[J]. Knowledge-based System, 2006, 19(7): 576-591

[7] Zhuowei L, Das A, Nandi S. Utilizing statistical characteristics of N-grams for intrusion detection [C]// Proc. of 2003 International Conf. on Cyberworlds. Oakland, CA, USA: IEEE Computer Society, 2003: 486-493

[8] 杜晔，王慧强，庞永刚. 一种基于均值 Hamming 距离的异常入侵检测方法[J]. 系统仿真学报，2004，16(12)：2853-2856

[9] Liao Y, Vemuri V R. Use of K-Nearest Neighbor classifier for intrusion detection[J]. Computer & Security, 2002, 21(5): 439-448

[10] Rawat S, Gulati V P, Pujari A K, et al. Intrusion Detection using Text Processing Techniques with a Binary-weighted Cosine Metric[J]. Journal of Information Assurance and Security, 2006, 1(1): 43-50

[11] Sharma A, Pujari A K, Paliwal K K. Intrusion detection using text processing techniques with a kernel based similarity measure[J]. Computer & Security, 2007, 26(7/8): 488-495

[12] Forrest S, Allen L, Perelson A S, et al. Self-nonself Discrimination in a Computer[C]// IEEE Symposium on Security and Privacy. Oakland, CA, USA: IEEE Computer Society, 1994: 202-213

[13] Kim J, Bentley P, Aickelin U, et al. Immune system approaches to intrusion detection-a review[J]. Natural Computing, 2007, 6(4): 413-466

[14] Wu Ying, Jiang Jianhui. Frequency Weighted Hamming Distance Based System Call Anomaly Detection[C]// Proc. of CSIE 2009. Los Angeles, California: IEEE Computer Society, 2009(1): 105-109

[15] D'haeseleer P, Forrest S, Helman P. An immunological approach to change detection: algorithms, analysis and implications [C]// Proc. of 1996 IEEE Symp. on Security and Privacy. Oakland, CA: IEEE Computer Society, 1996: 110-119

[16] Hofmeyr S A, Forrest S. Architecture for an Artificial Immune System[J]. Evolutionary Computation, 2000, 8(4): 443-473

[17] Matzinger P. The Danger Model: A Renewed Sense of Self[J]. Science, 2002, 296(5566): 301-305

[18] Aickelin U, Bentley P, Cayzer S, et al. Danger Theory: The link between AIS and IDS? [C]// The 2nd International Conference on Artificial Immune Systems. Edinburgh, UK, 2003: 147-155

[19] Iqbal A. Danger Theory Metaphor in Artificial Immune System for System Call Data[D]. Faculty of Computer Science and Information System, Universiti Teknologi Malaysia, 2006

[20] 尹清波，张汝波，李雪耀，等. 基于线性预测与马尔可夫模型的入侵检测技术研究[J]. 计算机学报，2005，28(5)：900-907

[21] Qiao Y, Xin X W, Bin Y, et al. Anomaly intrusion detection method based on HMM[J]. IEEE Electronic Letters, 2002, 38 (13): 663-664

[22] Rabiner L R, Juang B H. An Introduction to Hidden Markov Models[J]. IEEE ASSP Magazine, 1986, 3(1): 4-16

[23] Ye N, Li X, Chen Q, et al. Probabilistic Techniques for Intrusion Detection Based on Computer Audit Data[J]. IEEE Transactions on Systems, Man and Cybernetics-Part A: Systems and Humans, 2001, 31(4): 266-274

[24] Cho S, Park H. Efficient anomaly detection by modeling privilege flows using hidden Markov model[J]. Computer & Security, 2003, 22(1): 45-55

[25] Tokhtabayev A G, Skormin V A. Non-stationary Markov Models and Anomaly Propagation Analysis in IDS[C]// Third International Symp. on Information Assurance and Security. 2007: 203-208

[26] Hoang X D, Hu J. An Efficient Hidden Markov Model Training Scheme for Anomaly Intrusion Detection of Server Applications Based on System Calls[C]// Proc. of 12th IEEE International Conf. on Networks. IEEE Computer Society, 2004: 470-474

[27] Wang W, Guan X, Zhang X. Modeling Program Behaviors by Hidden Markov Model for Intrusion Detection[C]// Proc. of the 3rd International Conf. on Machine Learning and Cybernetics. Shanghai: IEEE Computer Society, 2004: 2830-2835

[28] Du Y, Wang H, Pang Y. A Hidden Markov Models-based Anomaly Intrusion Detection Method [C]// Proc. of 5th World Congress on Intelligent Control and Automation. Hangzhou, China: IEEE Computer Society, 2004: 4348-4351

[29] Han S, Cho S. Rule-based Integration of Multiple Measure-models for Effective Intrusion Detection[C]// Proc. of IEEE International Conf. on Systems. Man and Cybernetics. IEEE Computer Society, 2003: 120-125

[30] 谭小彬，王卫平，奚宏生，等. 计算机系统入侵检测的隐马尔可夫模型[J]. 计算机研究与发展，2003，40(2)：245-250

[31] 尹清波，张汝林，李雪耀，等. 基于动态马尔科夫模型的入侵检测技术研究[J]. 电子学报，2004，32(11)：1785-1788

[32] 张响亮，王伟，管晓宏. 基于隐马尔可夫模型的程序行为异常检测[J]. 西安交通大学学报，2005，39(10)：1056-1059

[33] 闫巧，谢维信，宋歌，等. 基于 HMM 的系统调用异常检测[J]. 电子学报，2003，31(10)：1486-1490

[34] Ghosh A K, Schwartzbard A, Schatz M. Learning program behavior profiles for intrusion detection[C]// Proc. of the Workshop on Intrusion Detection and Network Monitoring. Santa Clara, CA, USA, 1994

[35] Endler D. Intrusion detection: applying machine learning to solaris audit data [C]// Proc. of the 1998 Annual Computer Security Application Conf. Los Alamitos, CA: IEEE Computer Society, 1998: 268-279

[36] Rapaka A, Novokhodko A, Wunsch D. Intrusion Detection Using Rádial Basis Function Network on Sequences of System Calls[C]// Proc. of the International Joint Conf. on Neural Networks. IEEE Computer Society, 2003(3): 20-24

[37] Zhang X Q, Zhong L Z. Combining the HMM and the Neural Network Models to Recognize Intrusion[C]// Proc. of the Third International Conf. on Machine Learning and Cybernetics. Shanghai: IEEE Computer Society, 2004(2): 26-29

[38] 李千目，戚涌，张宏，等. IIDS 的行为特征提取方法研究[J]. 南京理工大学学报，2004，28(2)：140-144

[39] Chen W, Hsu S, et al. Application of SVM and ANN for intrusion detection[J]. Computer & Operations Research, 2005, 32 (10): 2617-2634

[40] Vapnik V. The Nature of Statistical Learning Theory[M]. New York: Springer Verlag, 1995

[41] Tian S, Mu S, Yin C. Sequence-similarity kernels for SVMs to detect anomalies in system calls[J]. Neurocomputing, 2007, 70 (4-6): 859-866

[42] Lee Y, Huang Y. Reduced Support Vector Machines: A Statistical Theory[J]. IEEE Transactions on Neural Networks, 2007, 18(1): 1-13

[43] Feng L, Wang W, Zhu L, et al. Predicting intrusion goal using dynamic Bayesian network with transfer probability estimation [J]. Journal of Network and Computer Applications, 2009, 32: 721-732

[44] Fayyad U, Piatetsky-Shapiro G, Smyth P. The KDD process of extracting useful knowledge from volumes of data[J]. Communications of the ACM, 1996, 39(11): 27-34

[45] Lee W, Stolfo S J. Data Mining Approaches for Intrusion Detection[C]// Proc. of the 7th USENIX Security Symp. Berkeley, CA, USA: SUENIX Association, 1998, 7: 6-16

[46] Lee W, Stolfo S J, Mok K W. Mining audit data to build intrusion detection models[C]// Proc. of the 4th International Conference on Knowledge Discovery and Data Mining. New York, USA: AAAI Press, 1998: 66-72

[47] Lee W, Stolfo S J, Mok K W. A Data Mining Framework for Building Intrusion Detection Model[C]// Proc. of 1999 IEEE Symp. on Security and Privacy. Los Alamitos, CA, USA: IEEE Computer Society, 1999: 120-132

[48] Li P, Park H, G Dao, et al. Bridging the Gap Between Data-flow and Control-flow Analysis for Anomaly Detection[C]// Proc. of the 24th Annual Computer Security Application Conference. Anaheim, California: IEEE Computer Society, 2008: 392-401

[49] 徐明，陈纯，应晶. 基于系统调用分类的异常检测[J]. 软件学报，2004，15(3)：391-403

[50] 刘海峰，卿斯汉，蒙扬，等. 一种基于审计的入侵检测模型及其实现机制[J]. 电子学报，2002，30(8)：1167-1171

[51] Kosoresow A P, Hofmeyr S A. Intrusion detection via system call traces[J]. IEEE Software, 1997, 14(5): 35-42

[52] Sekar R, Bendre M, Dhurjati D, et al. A Fast Automaton-based Method for Detecting Anomalous Program Behaviors [C]// Proc. of 2001 IEEE Symp. on Security and Privacy. Oakland, CA: IEEE Computer Society Press, 2001: 144-155

（下转第 47 页）

feedback vertex set of an interval graph [J]. Advanced Modeling and Optimization, 2005, 7(1): 99-116

[56] Kratsch D, Müller H, Todinca I. Feedback vertex set and longest induced path on AT-free graphs [G]// LNCS 2880: WG 2003. Berlin: Springer, 2003: 309-321

[57] Carrabs F, Cerulli R, Gentili M. Minimum weighted feedback vertex set on diamonds [J]. Information Processing Letters, 2005, 94(1)

[58] Chen Yenlian, Wang Y, Lee C. On the minimum weighted feedback vertex set problem on the parallel and serial connection of diamonds [C]// The 24th Workshop on Combinatorial Mathematics and Computation Theory. 2007

[59] Liang Y, Chang M. Minimum feedback vertex sets in cocomparability graphs and convex bipartite graphs [J]. Acta Informatica, 1997, 34: 337-346

[60] Coorg S, Rangan C. Feedback vertex set on cocomparability graphs [J]. Networks, 1995, 26: 101-111

[61] Cormen T, Leiserson C, Rivest R, et al. Introduction to Algorithms, Second Edition [M]. McGraw-Hill Book Company, Boston, MA, 2001

[62] Seymour P. Packing directed circuits fractionally [J]. Combinatorica, 1995, 15: 281-288

[63] Charbit P, Thomassé S, Yeo A. The Minimum Feedback Arc Set Problem is NP-Hard for Tournaments [J]. Combinatorics, Probability and Computing, 2007, 16: 1-4

[64] Alon N. Ranking tournaments [J]. SIAM Journal on Discrete Mathematics, 2006, 20(1): 37-142

[65] Ailon N, Charikar M, Newman A. Aggregating inconsistent information: ranking and clustering [C]//STOC 2005. New York: ACM, 2005

[66] Zuylen A. Deterministic approximation algorithms for clustering problems [R]. Ithaca, NY: School of Operations Research and Industrial Engineering, Cornell University, 2005

[67] Coppersmith D, Fleischer L, Rudra A. Ordering by weighted number of wins gives a good ranking for weighted tournaments [C]// SODA 2006. New York: ACM, 2006

[68] Guo Jiong, Hüffner F, Moser H. Feedback Arc Set in Bipartite Tournaments is NP-Complete [J]. Information Processing Letters, 2007, 102: 62-65

[69] Gupta S. Feedback Arc Set Problem in Bipartite Tournaments [J]. Information Processing Letters, 2008, 105: 150-154

[70] Chen Jianer, Kanj I, Meng Jie, et al. On the effective enumerability of NP problems [G]// LNCS 4169: IWPEC 2006. Berlin: Springer, 2006: 215-226

(上接第 25 页)

[53] Wagner D, Dean D. Intrusion Detection via Static Analysis [C]// Proc. of 2001 IEEE Symp. on Security and Privacy. Oakland, CA: IEEE Computer Society Press, 2001: 156-168

[54] Liu Z, Bridges S M, Vaughn R B. Combining Static Analysis and Dynamic Learning to Build Accurate Intrusion Detection Models [C]// Proc. of the 3rd IEEE International Workshop on Information Assurance. College Park, Maryland: IEEE Computer Society Press, 2005: 164-177

[55] Feng H, Kolesnikov O, Fogla P, et al. Anomaly detection using call stack information [C]// IEEE Symposium on Security and Privacy. Oakland, CA: IEEE Computer Society Press, 2003: 62-75

[56] Feng H H, Giffin J T, Huang Y, et al. Formalizing Sensitivity in Static Analysis for Intrusion Detection [C]// Proc. of 2004 IEEE Symp. on Security and Privacy. Oakland, CA: IEEE Computer Society Press, 2004: 194-208

[57] Giffin J T, Jha S, Miller B P. Efficient Context-sensitive Intrusion Detection [C]// 11th Annual Network and Distributed Systems Security Symposium. 2004

[58] 陆炜, 曾庆凯. 一种基于控制流的程序行为扩展模型[J]. 软件学报, 2007, 18(11): 2841-2850

[59] 李闻, 戴英侠, 连一峰, 等. 基于混杂模型的上下文相关主机入侵检测系统[J]. 软件学报, 2009, 20(1): 138-151

[60] Gopalakrishna R, Spafford E H, Vitek J. Efficient Intrusion Detection Using Automaton Inlining [C]// Proc. of 2005 IEEE Symp. on Security and Privacy. Oakland, CA: IEEE Computer Society Press, 2005: 18-31

[61] Esponda F, Forrest S, Helman P. A Formal Framework for Positive and Negative Detection Schemes [J]. IEEE Transactions on System, Man, and Cybernetics, PART B, 2004, 34(1): 357-373

[62] Lee W, Xiang D. Information-theoretic measures for anomaly detection [C]// Proc. of the 2001 IEEE Symp. on Security and Privacy. Oakland, CA: IEEE Computer Society Press, 2001: 130-143

[63] Tan K M C, Maxion R A. "Why 6?" defining the operational limits of stide, an anomaly-based intrusion detector [C]// Proc. of 2002 IEEE Symp. on Security and Privacy. Berkeley, CA: IEEE Computer Society Press, 2002: 173-186

[64] Esponda F, Forrest S, Helman P. Negative representations of information [J]. International Journal of Information Security, 2009, 8(5): 331-345

[65] Mutz D, Robertson W, Vigna G, et al. Exploiting Execution Context for the Detection of Anomalous System Calls [C]// Proc. of the 10th International Symposium on Recent Advances in Intrusion Detection. 2007

[66] Amer S H, Hamilton J A. Investigating intrusion detection systems that use trails of system calls [C]// Proc. of 2008 Inter. Symp. on Performance Evaluation of Computer and Telecommunication Systems. Edinburgh, UK, 2008: 377-384

[67] Hofmeyr S. The implications of immunology for secure systems design [J]. Computer & Security, 2004, 23(6): 453-455

[68] Mazeroff G, Gregor J, Thomason M, et al. Probabilistic suffix models for API sequence analysis of Windows XP applications [J]. Pattern Recognition, 2008, 41: 90-101.

[69] 朱莺嘤, 叶茂, 刘乃琦, 等. 一种基于图的异常入侵检测新算法[J]. 计算机科学, 2008, 35(11): 78-82

[70] 卿斯汉, 蒋建春, 马恒太, 等. 入侵检测技术研究综述[J]. 通信学报, 2004, 25(7): 19-29

[71] Forrest S, Hofmeyr S, Somayaji A. The Evolution of System-call Monitoring [C]// Proc. of the 24th Annual Computer Security Application conference. Anaheim, California: IEEE Computer Society, 2008: 418-430