(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 110618854 A
(43)申请公布日 2019.12.27

(21)申请号 201910772362.5

(22)申请日 2019.08.21

(71)申请人 浙江大学
地址 310058 浙江省杭州市西湖区余杭塘路866号

(72)发明人 吴春明 陈双喜 王婉飞 姜鑫悦 吴安邦

(74)专利代理机构 杭州求是专利事务所有限公司 33200
代理人 邱启旺

(51)Int.Cl.
G06F 9/455(2006.01)
G06F 21/56(2013.01)

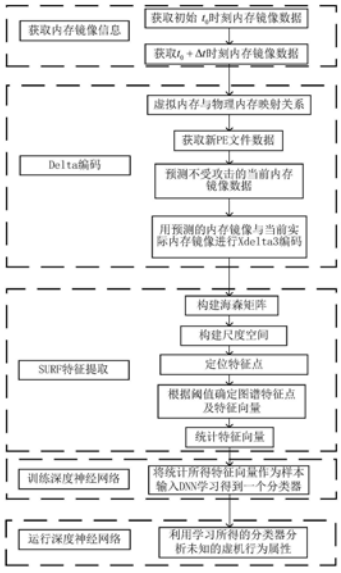
权利要求书2页 说明书6页 附图2页

(54)发明名称

基于深度学习与内存镜像分析的虚机行为分析系统

(57)摘要

本发明公开了一种基于深度学习与内存镜像分析的虚机行为分析系统，该系统通过获取内存镜像数据，进行delta编码，再对编码后的内存图谱提取图谱特征点信息，利用所得到的特征信息训练神经网络得到一个分类器，最后运行神经网络，利用得到的分类器分析未知的虚拟机行为。本发明操作简单，容易实现，便于模块化；本发明适用范围广，可用于检测已知攻击、未知攻击等多种攻击方式，即使攻击者潜伏一段时间后再发起攻击，也不会影响本发明的检测性能；此外，本发明在不同系统平台，都具有较好的鲁棒性、可靠性、可用性。



CN 110618854 A

1.一种基于深度学习与内存镜像分析的虚机行为分析系统,其特征在于,包括以下步骤:

(1)获取内存镜像数据,包括以下子步骤:

(1.1)在初始时刻t_0,使用内存取证工具获取初始内存镜像数据,得到初始内存。

(1.2)在任意时刻$t_0+\Delta t$,在VirtualBox,VMware虚拟化平台上,根据不同操作系统的内存管理机制,分别自动采样当前时刻各异构体不受攻击与受攻击情况下的内存镜像数据,得到当前内存,即正常样本与恶意样本。

(2)进行delta编码,包括以下子步骤:

(2.1)运行内存取证工具,对步骤(1.1)获取的初始内存使用pslist以及dlllist命令,分别确定初始内存中的EXE类型的可执行文件与DLL类型的动态链接库列表。

(2.2)对步骤(1.2)得到的当前内存运行内存取证工具中的pslist以及dlllist命令,分别确定当前内存中的EXE类型的可执行文件与DLL类型的动态链接库列表;

(2.3)分析步骤(2.1)和(2.2)得到的EXE类型的可执行文件与DLL类型的动态链接库列表,确定在当前内存中而不在初始内存中的可执行文件,称为新可执行文件;

(2.4)根据初始内存,为每一个新可执行文件生成一个预测内存,包括以下子步骤:

(2.4.1)确定每一个新可执行文件的进程ID,同时确定该进程在虚拟内存地址空间中的基地址;

(2.4.2)对于每一个新可执行文件的所属进程,根据步骤(2.4.1)中的进程基地址,在当前内存中运行内存取证工具中的memmap命令提取进程虚拟内存与物理内存的映射关系;

(2.4.3)将新可执行文件从虚拟磁盘上复制到初始内存中,对于新可执行文件的每个虚拟内存页,执行以下两步:首先,该虚拟内存页在当前内存中,使用步骤(2.4.2)中提取的虚拟内存与物理内存的映射关系,将新可执行文件复制到初始内存中;然后,记录页面复制信息,包括虚拟内存页的源页面位置、物理内存中目标页面位置、页面长度;最终生成预测内存;

(2.5)输出头信息,包括需要加载的新可执行文件的路径信息以及步骤(2.4.3)中提取的所有新可执行文件的页面复制信息;

(2.6)将步骤(2.4)生成的预测内存作为源,当前内存作为比较对象,使用xdelta3编码,得到当前内存镜像数据编码后的内存图谱;用M、N分别表示内存图谱的行数和列数,用I(i,j)=[a,b,c]表示内存图谱第i行第j列的元素;其中,$0\leqslant i<M$,$0\leqslant j<N$,a、b、c均为32位的浮点数,I(i,j)是一个三维向量;

(3)提取步骤(2.6)得到的内存图谱特征点信息,包括特征点位置、特征点大小、特征点的特征强度,包括以下子步骤:

(3.1)构建海森矩阵,具体为:计算内存图谱中每一个元素对应的海森矩阵H(i,j)的行列式,作为该元素的特征值,计算公式为:

$$\det(H(i,j))=D_{ii}\cdot D_{jj}-0.9D_{ij}\cdot D_{ij}$$

其中,$D_{ii}=I(i+1,j)+I(i-1,j)-2I(i,j)$,$D_{jj}=I(i,j+1)+I(i,j-1)-2I(i,j)$,$D_{ij}=I(i+1,j)+I(i,j-1)-2I(i,j)$;

(3.2)采用SURF的方式构建尺度空间:首先采用9×9的盒子滤波器对内存图谱原图像进行滤波处理,作为最底层的图像;然后逐渐增大盒子滤波器的尺寸,对内存图谱原图像继

续进行滤波处理;最终得到不同尺度的滤波响应图,构造尺度空间;所述尺度空间有4层,层与层之间的缩放比率为2;

(3.3)精确定位特征点,具体为:在每一个3×3×3的局部区域中,对步骤(3.2)构建的尺度空间进行非最大值抑制;将尺度空间中每一个元素与其三维邻域的26个元素的特征值进行比较,其中特征值比周围26个元素都大或者都小的元素为特征点,记录特征点位置(i,j)及尺度s;

(3.4)根据阈值确定图谱特征点及特征向量,具体为:比较步骤(3.3)得到的每个特征点在相应尺度下的特征值与预设的阈值,如果对应的特征值小于预设的阈值,则该特征点不作为最终特征点;如果对应的特征值大于等于预设的阈值,则将该特征点作为最终特征点,特征向量表示为[i,j,s,det(H(i,j,s))];其中,i、j是最终特征点在内存图谱中的行号与列号,s是最终特征点对应的滤波器尺度,det(H(i,j,s))是最终特征点在尺度s下的特征值;

(3.5)统计特征向量,具体为:判断步骤(3.4)得到的特征向量的来源,所述来源包括步骤(1.2)中不受攻击情况下的内存镜像数据和受攻击情况下的内存镜像数据;确定每个特征向量对应的标签z,用z=0表示该特征向量来源于不受攻击情况下的内存镜像数据,用z=1表示该特征向量来源于受攻击情况下的内存镜像数据;最终得到特征向量序列[i,j,s,det(H(i,j,s)),z];

(4)训练神经网络,具体为:将步骤(3.5)得到的特征向量序列作为深度神经网络的输入样本,以虚拟机行为是否正常为输出,训练深度神经网络得到一个虚拟机行为分类器;

(5)运行神经网络,分析未知的虚拟机行为,具体为:用步骤(4)得到的虚拟机行为分类器对运行状态未知的虚拟机进行分析,判断未知的虚拟机行为是否正常。

2.根据权利要求1所述基于深度学习与内存镜像分析的虚机行为分析系统,其特征在于,所述步骤(1.1)中初始时刻t_0为正实数。

3.根据权利要求1所述基于深度学习与内存镜像分析的虚机行为分析系统,其特征在于,所述步骤(1.2)中Δt为正实数。

4.根据权利要求1所述基于深度学习与内存镜像分析的虚机行为分析系统,其特征在于,所述步骤(1.2)中,对于正常样本,采用常用的内存镜像手段即可得到;对于恶意样本,为所有的异构执行体开辟共享空间存放不同种类的恶意工具样本,为所有异构执行体配置模拟入侵环境,从而得到虚拟化平台受不同类型攻击时的内存镜像数据。

5.根据权利要求1所述基于深度学习与内存镜像分析的虚机行为分析系统,其特征在于,所述步骤(3.3)中一个元素三维邻域的26个元素指与该元素在同一尺度上的8个元素和在其之上及之下的两个尺度层的9个元素。

6.根据权利要求1所述基于深度学习与内存镜像分析的虚机行为分析系统,其特征在于,所述步骤(3.4)中预设的阈值取决于要识别的特征数量,阈值设定越高,能识别的特征就越少。

7.根据权利要求1所述基于深度学习与内存镜像分析的虚机行为分析系统,其特征在于,所述步骤(4)中深度神经网络为任意一种现有的深度神经网络结构。

基于深度学习与内存镜像分析的虚机行为分析系统

技术领域

[0001] 本发明属于无线网络安全领域，具体是拟态主动防御领域，涉及一种基于深度学习与内存镜像分析的虚机行为分析系统。

背景技术

[0002] 虚拟化的云平台是云计算的重要部分。虚拟化的云平台是指在同一云平台上同时运行多个操作系统，每个系统拥有自己独立的运行空间。通过一台服务器上运行多台虚拟服务器，提高了机器的使用效率，从而减小硬件采购开支，是打造绿色数据中心的重要方式。基于虚拟机的云平台使用户能自主搭建自己的业务环境，运行稳定且具有良好的扩展性与迁移性，在金融行业、零售行业、数字营销、教育行业、政企单位等领域中应用广泛。

[0003] 虚拟化的云平台结构具有开放特性，由此衍生出一系列与虚拟机相关的安全问题。虚拟机中运行的资源数据以及应用容易受到入侵者的损害。因此，虚拟机需要更多的安全保障机制来加速大规模云服务的部署。其中首要问题是如何实时正确地判断虚拟机行为，判断虚拟机是否遭受恶意攻击。

[0004] 目前，解决虚机运行安全的方法有：基于网络流数据、基于日志、基于先验知识的虚机运行状态判断方法。基于网络流数据的虚机行为判断方法通过判断虚拟机网卡接收的数据是否含恶意数据包，检测虚拟机是否遭受恶意攻击。这种方法需要通信协议可解析，无法应对未知协议。另外，利用大量的数据包导致该判断方法计算开销较大。基于日志分析的方法通过分析虚拟机系统日志判断虚拟机是否遭受恶意攻击。但是日志本身具有滞后性，往往系统需要判断一系列的活动与动作才能判定入侵的发生，这对于即使阻止活跃的入侵行为是十分不利的。基于先验知识的判断方法需要已知攻击行为，无法应对未知漏洞、未知后门、未知攻击。

[0005] 为了实时保证虚拟机的安全性，亟需一种不依赖于已漏洞库、攻击库，且快速有效的虚机行为分析方法，以提高威胁发现的准确性和效率，实现虚拟机的可靠性、可用性、安全性。

发明内容

[0006] 本发明的目的在于针对现有技术的不足，提供一种基于深度学习与内存镜像分析的虚机行为分析系统。本发明针对网络中的内部攻击与外部攻击、已知攻击与未知攻击，保证虚拟机平台的安全性，对未知威胁及时作出预警，能正确实时地判断虚拟机行为，提高云虚拟机的安全性、可靠性、可用性。

[0007] 本发明的目的是通过以下技术方案来实现的：一种基于深度学习与内存镜像分析的虚机行为分析系统，包括以下步骤：

[0008] (1)获取内存镜像数据，包括以下子步骤：

[0009] (1.1)在初始时刻t_0，使用内存取证工具获取初始内存镜像数据，得到初始内存。

[0010] (1.2)在任意时刻$t_0+\Delta t$，在VirtualBox，VMware虚拟化平台上，根据不同操作系

统的内存管理机制,分别自动采样当前时刻各异构体不受攻击与受攻击情况下的内存镜像数据,得到当前内存,即正常样本与恶意样本。

[0011] (2)进行delta编码,包括以下子步骤:

[0012] (2.1)运行内存取证工具,对步骤(1.1)获取的初始内存使用pslist以及dlllist命令,分别确定初始内存中的EXE类型的可执行文件与DLL类型的动态链接库列表。

[0013] (2.2)对步骤(1.2)得到的当前内存运行内存取证工具中的pslist以及dlllist命令,分别确定当前内存中的EXE类型的可执行文件与DLL类型的动态链接库列表;

[0014] (2.3)分析步骤(2.1)和(2.2)得到的EXE类型的可执行文件与DLL类型的动态链接库列表,确定在当前内存中而不在初始内存中的可执行文件,称为新可执行文件;

[0015] (2.4)根据初始内存,为每一个新可执行文件生成一个预测内存,包括以下子步骤:

[0016] (2.4.1)确定每一个新可执行文件的进程ID,同时确定该进程在虚拟内存地址空间中的基地址;

[0017] (2.4.2)对于每一个新可执行文件的所属进程,根据步骤(2.4.1)中的进程基地址,在当前内存中运行内存取证工具中的memmap命令提取进程虚拟内存与物理内存的映射关系;

[0018] (2.4.3)将新可执行文件从虚拟磁盘上复制到初始内存中,对于新可执行文件的每个虚拟内存页,执行以下两步:首先,该虚拟内存页在当前内存中,使用步骤(2.4.2)中提取的虚拟内存与物理内存的映射关系,将新可执行文件复制到初始内存中;然后,记录页面复制信息,包括虚拟内存页的源页面位置、物理内存中目标页面位置、页面长度;最终生成预测内存;

[0019] (2.5)输出头信息,包括需要加载的新可执行文件的路径信息以及步骤(2.4.3)中提取的所有新可执行文件的页面复制信息;

[0020] (2.6)将步骤(2.4)生成的预测内存作为源,当前内存作为比较对象,使用xdelta3编码,得到当前内存镜像数据编码后的内存图谱;用M、N分别表示内存图谱的行数和列数,用I(i,j)=[a,b,c]表示内存图谱第i行第j列的元素;其中,$0\leqslant i<M$,$0\leqslant j<N$,a、b、c均为32位的浮点数,I(i,j)是一个三维向量;

[0021] (3)提取步骤(2.6)得到的内存图谱特征点信息,包括特征点位置、特征点大小、特征点的特征强度,包括以下子步骤:

[0022] (3.1)构建海森矩阵,具体为:计算内存图谱中每一个元素对应的海森矩阵H(i,j)的行列式,作为该元素的特征值,计算公式为:

[0023] $\det(H(i,j))=D_{ii}\cdot D_{jj}-0.9D_{ij}\cdot D_{ij}$

[0024] 其中,$D_{ii}=I(i+1,j)+I(i-1,j)-2I(i,j)$,$D_{jj}=I(i,j+1)+I(i,j-1)-2I(i,j)$,$D_{ij}=I(i+1,j)+I(i,j-1)-2I(i,j)$;

[0025] (3.2)采用SURF的方式构建尺度空间:首先采用9×9的盒子滤波器对内存图谱原图像进行滤波处理,作为最底层的图像;然后逐渐增大盒子滤波器的尺寸,对内存图谱原图像继续进行滤波处理;最终得到不同尺度的滤波响应图,构造尺度空间;所述尺度空间有4层,层与层之间的缩放比率为2;

[0026] (3.3)精确定位特征点,具体为:在每一个3×3×3的局部区域中,对步骤(3.2)构

建的尺度空间进行非最大值抑制;将尺度空间中每一个元素与其三维邻域的26个元素的特征值进行比较,其中特征值比周围26个元素都大或者都小的元素为特征点,记录特征点位置(i,j)及尺度s;

[0027] (3.4)根据阈值确定图谱特征点及特征向量,具体为:比较步骤(3.3)得到的每个特征点在相应尺度下的特征值与预设的阈值,如果对应的特征值小于预设的阈值,则该特征点不作为最终特征点;如果对应的特征值大于等于预设的阈值,则将该特征点作为最终特征点,特征向量表示为[i,j,s,det(H(i,j,s))];其中,i、j是最终特征点在内存图谱中的行号与列号,s是最终特征点对应的滤波器尺度,det(H(i,j,s))是最终特征点在尺度s下的特征值;

[0028] (3.5)统计特征向量,具体为:判断步骤(3.4)得到的特征向量的来源,所述来源包括步骤(1.2)中不受攻击情况下的内存镜像数据和受攻击情况下的内存镜像数据;确定每个特征向量对应的标签z,用z=0表示该特征向量来源于不受攻击情况下的内存镜像数据,用z=1表示该特征向量来源于受攻击情况下的内存镜像数据;最终得到特征向量序列[i,j,s,det(H(i,j,s)),z];

[0029] (4)训练神经网络,具体为:将步骤(3.5)得到的特征向量序列作为深度神经网络的输入样本,以虚拟机行为是否正常为输出,训练深度神经网络得到一个虚拟机行为分类器;

[0030] (5)运行神经网络,分析未知的虚拟机行为,具体为:用步骤(4)得到的虚拟机行为分类器对运行状态未知的虚拟机进行分析,判断未知的虚拟机行为是否正常。

[0031] 进一步地,所述步骤(1.1)中初始时刻t_0为正实数。

[0032] 进一步地,所述步骤(1.2)中Δt为正实数。

[0033] 进一步地,所述步骤(1.2)中,对于正常样本,采用常用的内存镜像手段即可得到;对于恶意样本,为所有的异构执行体开辟共享空间存放不同种类的恶意工具样本,为所有异构执行体配置模拟入侵环境,从而得到虚拟化平台受不同类型攻击时的内存镜像数据。

[0034] 进一步地,所述步骤(3.3)中一个元素三维邻域的26个元素指与该元素在同一尺度上的8个元素和在其之上及之下的两个尺度层的9个元素。

[0035] 进一步地,所述步骤(3.4)中预设的阈值取决于要识别的特征数量,阈值设定越高,能识别的特征就越少。

[0036] 进一步地,所述步骤(4)中深度神经网络为任意一种现有的深度神经网络结构。

[0037] 本发明的有益效果是:本发明利用内存镜像数据分析与深度学习机制,通过内存镜像数据的编码特征分析虚拟机行为属性;与已有虚拟平台状态分析方法相比,本发明操作简单,容易实现,便于模块化;本发明适用范围广,可用于检测已知攻击、未知攻击等多种攻击方式,即使攻击者潜伏一段时间后再发起攻击,也不会影响本发明的检测性能;此外,本发明在不同系统平台,都具有较好的鲁棒性、可靠性、可用性。

附图说明

[0038] 图1为本发明实施例中的系统模型示意图;

[0039] 图2为本发明方法的流程图。

具体实施方式

[0040] 下面结合附图并举实施例对本发明的技术方案进行详细说明。

[0041] 考虑到内存镜像数据能完整表示一台虚拟机的运行状态,因此,本发明利用内存镜像数据,结合深度神经网络,提出了一种基于深度学习与内存镜像分析的虚机行为分析系统。

[0042] 如附图1所示,本实施例系统模型为:在一个虚拟平台上运行多个操作系统,包括WinServer、Ubuntu、CentOS、RedHat。通过人工手段向各个操作系统导入后门、病毒恶意工具数据库,可以随时获得各个系统不受攻击时的内存镜像数据与受到不同类型攻击后的内存镜像数据。本方法将利用这些数据通过内存图谱编码提取内存数据特征,进而利用内存特征判断虚机行为状态是否受到攻击,流程如附图2所示,具体包括以下步骤:

[0043] 步骤一、获取内存镜像数据;具体过程如下:

[0044] (1)在初始时刻$t_0=0$,使用内存取证工具获取初始内存镜像数据;

[0045] (2)经过$\Delta t=1$时间,在VirtualBox,VMware虚拟化平台上,根据不同操作系统的内存管理机制,分别自动采样当前时刻各异构体正常情况(不受攻击)与受攻击情况下的内存镜像数据,即正常样本与恶意样本。对于正常样本,采用常用的内存镜像手段即可实现;对于恶意样本,为所有的异构执行体开辟共享空间存放不同种类的恶意工具样本,为所有异构执行体配置模拟入侵环境,从而得到虚拟平台受不同类型攻击时的内存镜像数据;

[0046] 步骤二、进行delta编码;具体过程如下:

[0047] (1)运行内存取证工具,对初始化的内存使用pslist以及dlllist命令分别确定初始化内存中的EXE类型的可执行文件与DLL类型的动态链接库列表;

[0048] (2)对当前的内存运行内存取证工具中的pslist以及dlllist命令分别确定当前内存中的EXE类型的可执行文件与DLL类型的动态链接库列表;

[0049] (3)分析上两步得到的EXE/DLL列表,确定在当前内存中而不在初始内存中的可执行(portable executable,PE)文件;

[0050] (4)根据初始内存,为每一个新的PE生成一个预测内存;

[0051] a)确定每一个新PE的进程ID,同时确定该进程在虚拟内存地址空间中的基地址;

[0052] b)对于每一个新PE的所属进程,在当前内存中运行内存取证工具中的memmap命令提取进程虚拟内存与物理内存的映射关系;

[0053] c)将新PE从虚拟磁盘上的对应文件复制到初始内存中;对于PE文件的每个虚拟内存页,执行以下两步:首先,如果该页在当前内存中,使用步骤二中(4)b)中得到的虚拟内存与物理内存映射关系,将PE文件复制到初始内存中;第二,记录页面复制信息,包括PE文件中源页面位置、物理内存中目标页面位置、页面长度;

[0054] (5)输出头信息,包括需要加载的新PE的路径信息以及每个PE的所有拷贝页面;

[0055] (6)将预测的内存作为源、当前内存作为比较对象,使用xdelta3编码,得到当前内存镜像数据编码后的内存图谱;用M,N分别表示图谱的行数和列数,用$I(i,j)=[a,b,c]$表示图谱第i行第j列的元素,$0\leq i<M$,$0\leq j<N$,a,b,c均为32位的浮点数,$I(i,j)$是一个三维向量;

[0056] 步骤三、提取内存图谱特征点信息,包括特征点位置、特征点大小、特征点的特征强度;具体过程如下:

[0057] (1)构建Hessian矩阵；

[0058] Hessian矩阵是特征提取算法的核心算子。任意一个二元函数f(x,y)的Hessian矩阵H表示为：

[0059] $$H\left(f\left(x,y\right)\right)=\begin{bmatrix}\frac{\partial^2 f}{\partial x^2} & \frac{\partial^2 f}{\partial x\partial y}\\ \frac{\partial^2 f}{\partial x\partial y} & \frac{\partial^2 f}{\partial y^2}\end{bmatrix};$$

[0060] 用矩阵H的行列式表示f(x,y)的特征值：

[0061] $$\det\left(\mathbf{H}\left(f\left(x,y\right)\right)\right)=\frac{\partial^2 f}{\partial x^2}\frac{\partial^2 f}{\partial y^2}-\left(\frac{\partial^2 f}{\partial x\partial y}\right)^2;$$

[0062] 对于特征提取过程，为加快实际应用中的计算速度，采用近似的方式求解海森矩阵，内存镜像图谱中第i行第j列的元素对应的海森矩阵H(i,j)的行列式计算为：

[0063] $\det(H(i,j))=D_{ii}\cdot D_{jj}-0.9D_{ij}\cdot D_{ij}$；

[0064] 其中，·表示向量点积，即各元素乘积之和，$D_{ii}=I(i+1,j)+I(i-1,j)-2I(i,j)$，$D_{jj}=I(i,j+1)+I(i,j-1)-2I(i,j)$，$D_{ij}=I(i+1,j)+I(i,j-1)-2I(i,j)$；

[0065] 对内存镜像图谱中的每一个元素都做上述计算，得到图谱中每一个像素点的对应海森矩阵的行列式，即该像素点的特征值；

[0066] (2)构建尺度空间；

[0067] 尺度空间是一幅图谱在不同解析度下的表示；为了模拟图像数据的多尺度特征，在空间域与尺度域上找到极值点，确定初步的特征点，需要为图谱构建尺度空间，通过多次重复的二元函数与高斯函数核卷积构建图谱在不同尺度域上的特征值；

[0068] 本专利采用SURF的方式构建尺度空间；对于任意一张内存镜像图谱，都保持原图像大小不变，通过改变模板盒子尺寸对原图像进行滤波，构造出尺度空间；同时，SURF可以采用并行运算，对尺度空间中的各层图像同时进行处理；通过逐渐增大的盒子尺寸滤波模板与积分图像卷积，由各像素点对应的Hessian矩阵行列式得到响应图像，构造出金字塔；

[0069] 首先采用9×9的盒子滤波器得到的响应图像作为最底层的图像，然后逐渐增大盒子的尺寸，对原图像继续进行滤波处理；将尺度空间划分为4层，层与层之间的缩放比率为2，每一层包含不同尺度的滤波响应图；每层都是采用逐渐增大的滤波器尺寸进行处理，从而得到含有多层的一系列不同尺度的图谱；

[0070] (3)精确定位特征点；

[0071] 在每一个3×3×3的局部区域中，进行非最大值抑制；对于每一个像素点，与同一尺度上的8个点和在其之上及之下的两个尺度层9个点进行比较，只有比周围的26个领域值都大或者都小的极值点才能作为特征点，记录特征点位置(i,j)及尺度s；

[0072] (4)根据阈值确定图谱特征点及特征向量；

[0073] 对上一步中得到的每个特征点，比较该点在相应尺度下的特征值与预设的阈值。如果对应的特征值小于预设的阈值，则该点无法作为特征点；如果对应的特征值大于等于预设的阈值，则该点可以作为最终特征点，特征向量表示为[i,j,s,det(H(i,j,s))]，其中，i,j是该特征点在图谱中得行号与列号，s是该点可以作为特征点时对应的滤波器尺度，det

(H(i,j,s))是该点在尺度s下的特征值；

[0074] (5)统计特征向量；

[0075] 对于上一步得到的特征向量，根据其来源，即来源于不受攻击的内存镜像数据还是受攻击的内存镜像数据，为每个特征向量确定对应的标签z，用z＝0表示该特征向量来源于不受攻击的内存镜像数据，用z＝1表示该特征向量来源于受攻击的内存镜像数据；

[0076] 至此，Delta编码后的内存图谱通过特征提取，内存图谱抽象成为特定编码的带标签的特征向量序列；

[0077] 步骤四、训练神经网络；

[0078] 深度神经网络的一个输入样本表示为[i,j,s,det(H(i,j,s)),z]；选用一种现有的深度神经网络结构训练得到一个分类器，用于实际运行时分析未知虚拟机行为；

[0079] 步骤五、运行神经网络，分析未知的虚拟机行为；

[0080] 用步骤四训练好的神经网络对运行状态未知的虚拟机进行分析，判断未知的虚拟机行为是否正常。

[0081] 以上所述为本发明的一个实施例，本发明不受上述实施例限制，可将本发明的技术方案与实际应用场景结合确定具体实施方法。

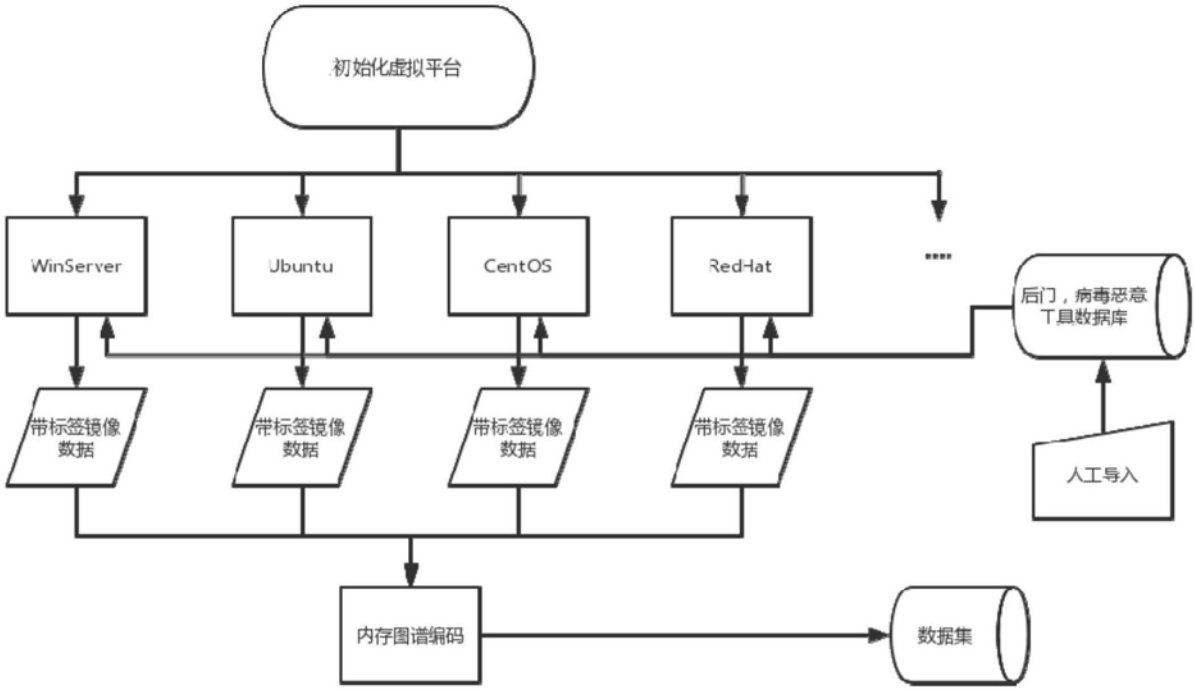

初始化虚拟平台
WinServer
Ubuntu
CentOS
RedHat
....
后门，病毒恶意
工具数据库
带标签镜像
数据
带标签镜像
数据
带标签镜像
数据
带标签镜像
数据
人工导入
内存图谱编码
数据集

图1

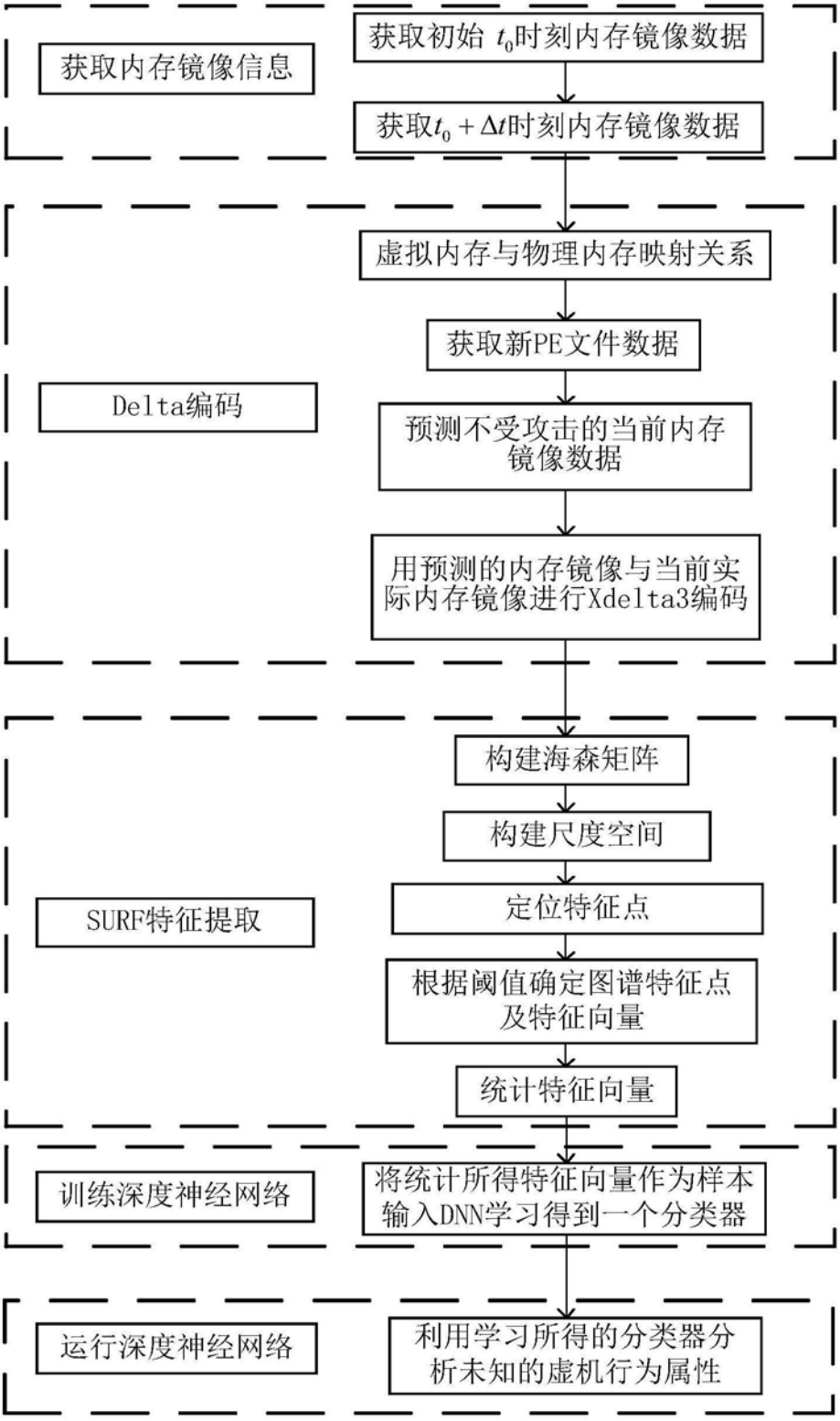

获取内存镜像信息
获取初始 t_0时刻内存镜像数据
获取$t_0+\Delta t$时刻内存镜像数据
虚拟内存与物理内存映射关系
获取新PE文件数据
Delta编码
预测不受攻击的当前内存镜像数据
用预测的内存镜像与当前实际内存镜像进行Xdelta3编码
构建海森矩阵
构建尺度空间
SURF特征提取
定位特征点
根据阈值确定图谱特征点及特征向量
统计特征向量
训练深度神经网络
将统计所得特征向量作为样本输入DNN学习得到一个分类器
运行深度神经网络
利用学习所得的分类器分析未知的虚机行为属性

图2