基于业务用户行为的计算机动态取证评估模型研究

王丹琛[1,2]，张仕斌[3]，徐 扬[1]，许 宁[2]

(1. 西南交通大学智能控制开发中心 成都 610031; 2. 四川省信息安全测评中心 成都 610017;
3. 成都信息工程大学信息安全工程学院 成都 610225)

【摘要】对复杂信息系统的业务用户行为和网络取证进行了研究，结合木马技术提出了基于业务用户行为的计算机动态取证评估模型，该模型构建了基于云模型的业务用户行为定量评估方法。通过仿真实验验证了模型评估的合理性，同时验证了该模型能实时隐蔽地记录用户行为，并能确保将获取的信息反馈给取证控制端，为计算机动态取证的研究提供了一种可行的技术方案。

关 键 词 行为评估; 业务用户行为; 云模型; 计算机动态取证; 信任云
中图分类号 TP393.08 **文献标志码** A doi:10.3969/j.issn.1001-0548.2015.06.022

Study on the Dynamic Computer Forensic Evaluation Model Based on Business User's Behavior

WANG Dan-chen[1,2], ZHANG Shi-bin[3], XU Yang[1], and XU Ning[2]

(1. Intelligent Control Development Center, Southwest Jiao tong University Chengdu 610031;
2. Sichuan Information Security Testing Evaluation Center Chengdu 610017;
3. College of Information Engineering, Chengdu University of Information Technology Chengdu 610225)

Abstract A dynamic computer forensic model based on business user's behavior is proposed under the research background of complex network environment of information system. This model, which adopts the Trojans theory, provides a method of quantitative evaluation of business user's behavior based on cloud model theory. The rationality of the model's evaluation is verified through simulation tests. At the meantime, it is proved that the model is able to record the business user's behavior covertly and real-timely, and ensure that the obtained evidence can be fed beck to the control terminal, offering a feasible technical approach to the research of computer forensics.

Key words behavior evaluation; business user behavior; cloud model theory; dynamic computer forensic; trust cloud

网络用户行为作为网络行为学研究的内容之一，其本质就是研究网络上用户行为的规律和特点，最终达到控制或预测用户行为[1-2]。通过对网络用户行为以及网络取证的研究与分析，发现在网络犯罪领域，对网络中不安全的用户行为进行实时取证，对于打击网络犯罪，推动计算机动态取证的发展具有重要的现实意义。当前，计算机取证及安全评估研究吸引了众多研究者，取得了一些重要研究成果。文献[3]主要在取证中将不同的隐私级别赋予不同保护机制，能够有效缓和隐私保护和计算机取证之间的矛盾，使取证得到的证据能够更加合法；文献[4]将哈希算法用于电子证据的保存中，提出了保证电子证据的完整性提出一种新的解决方案；文献[5]引入模糊神经网络来检测正常和异常的网络流量，以及时地阻止不安全的行为，设计了一种基于模糊神经网络的取证模型；文献[6]使用多代理机制分层进行检测与分析，提出一个协作的多智能体的取证工具；文献[7]采用多线程和虚拟技术对捕获的数据进行审计与分析，设计了一种基于入侵检测和防火墙技术的联动取证系统；文献[8]利用Multi-Agent技术的自主学习和推理能力，设计一种基于Multi-Agent的取证系统，各Agent相互协调与合作，共同完成对网络取证；文献[9]提出了一种新的磁盘映像模式，将更多的电子证据和调查程序共享在虚拟电子证据

收稿日期：2014－03－12；修回日期：2014－12－23
基金项目：国家自然科学基金(61175055)；四川省重点科技研究发展计划(2011FZ0051)；工信部无线电管理局项目([2011]146)
作者简介：王丹琛(1982－)，女，博士，主要从事基于业务信息系统安全评估及智能信息处理方面的研究.

图书馆(VEEL)中；文献[10]借助于云模型理论，设计了一种基于云模型的计算机取证系统。

通过对上述取证相关模型及理论与技术的分析发现，上述研究成果尚存在一些不足，如：在网络取证中，没有深入分析网络业务用户行为；取证过程中不能保证取证程序的隐蔽性且缺乏保证证据安全的有效措施；获取的数据针对性差，大多数据是无用的。基于以上原因，本文借鉴已有研究工作，结合作者在文献[11-13]中的研究成果，以复杂信息系统的网络环境为研究背景，引入云模型理论对网络业务用户行为进行研究并定量描述，研究并提出了基于业务用户行为的动态取证评估模型。

1 计算机取证与网络行为的研究

1.1 计算机取证的相关问题

在计算机取证发展的初期一般均为静态取证，磁盘镜像技术、数据恢复技术、信息过滤技术等有了很大的进展，一些工具也陆续问世[8](如Quick View Plus和ThumbsPlus)。动态取证通过对计算机或网络系统进行监控，实时获取并分析相关信息；网络取证[10]主要针对的是计算机动态取证，它更强调现场监控，实时地收集网络中的信息和通过诱骗等技术对网络实施主动防御。

1.2 网络行为的相关问题

以往研究网络行为主要侧重于对网络流量进行分析；随着技术的发展，人们意识到虽然网络中行为形式各异，但同一用户的长期行为呈现一定的趋势，分析这些趋势能基本得到该用户在网上的活动范围。

业务用户行为分析的过程如图1所示。由于建模方法不同，导致分析过程中存在一些差异，用户行为也表现出不同的形式，因而对用户行为实施后续操作也将随之改变。

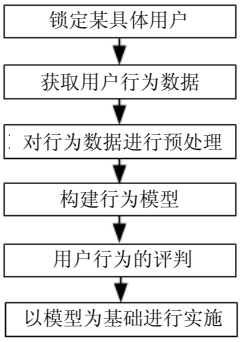

图1 业务用户行为分析过程

2 基于业务用户行为的动态取证模型

2.1 基于业务用户行为的计算机动态取证的思路

基于业务用户行为的计算机动态取证模型包括用户行为评估和计算机动态取证模型，如图2所示。模型在用户行为评估模型的基础上结合木马技术来构建，该模型能够对不安全的用户行为进行实时取证，最终能确保网络的安全和实时取证。

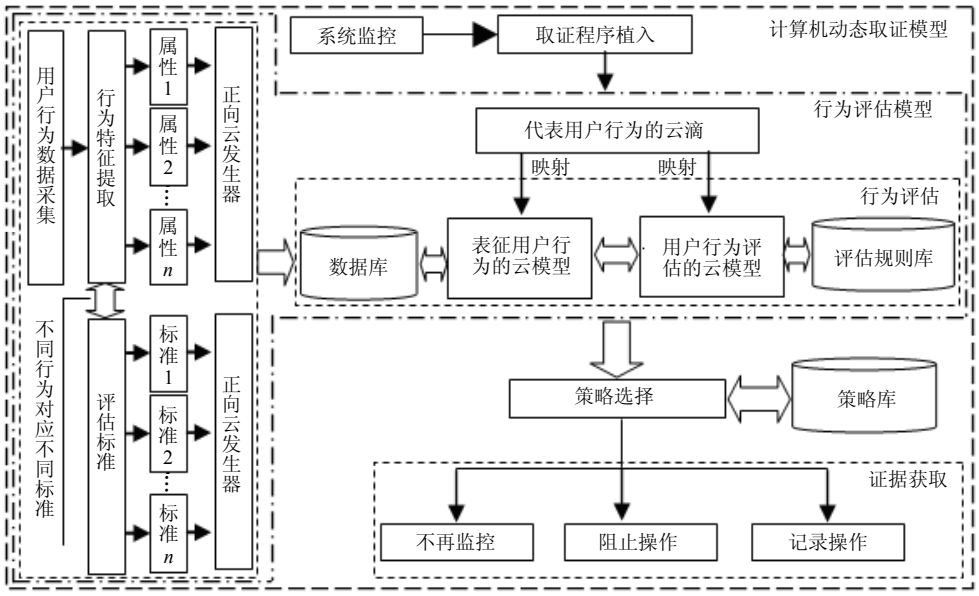

图2 构建基于业务用户行为的计算机动态取证模型的思路

2.2 基于云模型的业务用户行为评估模型

在复杂信息系统的网络环境中，业务用户行为的不确定性与云模型理论的基本特征吻合，故本文拟借助于云模型理论对业务用户行为进行描述(构

建业务用户行为模型)；为了体现对不同用户行为评估的差异性，本文也借助于云模型理论对用户行为进行评估(构建行为评估模型)。

2.2.1 云模型理论的相关基础

定义 1 设$U=\{x\}$是定量域，C代表定性概念，$f(x)$($f(x)\in[0,1]$)代表U到C的随机映射关系且具有某种稳定倾向，则x在U上的分布就称为云，每一个x就是一个云滴[12]。

为了将定性的概念按定量的方式进行描述，云用期望(Ex)、熵(En)、超熵(He)3个数字特征来表征一个定性概念的整体特征[14]。

定义 2 正向云发生器[11]：将定性概念转换成定量的描述，由云的数字特征产生云滴。

定义 3 逆向云发生器[11]：是正向云发生器的逆过程，是由云滴得到云的数字特征的过程。

2.2.2 基于云模型理论的业务用户行为评估模型

本文拟应用云模型理论[14]的3个数字特征(Ex,En,He)对复杂信息系统的网络环境中不确定的用户行为进行定量描述和评估。

1) 基于云模型理论的业务用户行为模型

设用户行为属性集为$U=\{U_1,U_2,\cdots,U_n\}$，$U_i(i=1,2,\cdots,n)$为一次用户整体行为，令$U_i=\{\mathrm{Ex}_i,\mathrm{En}_i,\mathrm{He}_i\}$代表一次用户行为的数字特征(其中，$\mathrm{Ex}_i$反映了用户行为的整体特征；$\mathrm{En}_i$反映了用户行为的不确定性；$\mathrm{He}_i$反映了$\mathrm{En}_i$的不确定性)。考虑到各行为属性对用户整体行为的影响不同，因而各行为属性在整体行为中所占的比重也不相同。如用BW_{U_i}表示一次行为的权重(在不同网络环境中，各网络业务用户行为的权重是不同的，故BW_{U_i}的值可根据实际情况来设定)。由于Ex_i是对行为最直接的量化，为了与客观事实更为接近，在此用式(1)来代表描述用户行为的期望。

$$\mathrm{Ex}_i'=\mathrm{BW}_{U_i}\times\mathrm{Ex}_i \tag{1}$$

2) 基于云模型理论的业务用户行为评估模型

设评估标准集为$C=\{C_1,C_2,\cdots,C_n\}$，其中，$C_i=(\mathrm{Ex}_{U_i},\mathrm{En}_{U_i},\mathrm{He}_{U_i})$是对$U_i$评估的标准集的数字特征，体现了对不同用户行为评估标准的差异性。为了体现评估主体的影响，评估主体事先设置好容忍度[11]；然后以评估标准集为依据得到评估该用户行为的数字特征；最后由正向云发生器转换得到该行为评估的云模型，完成业务用户行为评估。

2.2.3 基于云模型理论的业务用户行为评估过程

1) 计算单次用户行为的可信得分

当用户进行一次操作时，可以得到一个表征其行为的数值x_i，将该值映射到表征用户一次行为的云模型中，可以得到其行为确定度值$u(x_i)$($u(x_i)$即是云的定义中的$f(x)$，x_i是用户本次操作直接获得的数值，而$x_iu(x_i)$是实际值乘以云模型的确定度值后的修正值，代表本次行为在云模型中表现出来的行为可能性趋势)。

由文献[11]中可信得分的定义，按一定的规则(根据用户行为评估标准集具体设定)计算出x_i和$x_iu(x_i)$对应的可信得分s_i和s_{i+1}，然后将其映射到云模型中并评估业务用户行为，可以得到其行为的确定度值$f_i(x)$和$f_{i+1}(x)$，再由式(2)计算出该次行为的确定度值$c_i(x_i)$，最后由式(3)计算出该次行为的可信得分。

$$c_i(x_i)=\frac{f_i(x)+f_{i+1}(x)}{2} \tag{2}$$

$$s_i(x_i)=\frac{s_i+s_{i+1}}{2} \tag{3}$$

1) 用户整体行为可信得分的计算

由于评估用户整体行为各属性的重要程度不同，可结合权重计算出用户整体行为确定度值TC和整体行为的可信得分TS，具体计算公式如下：

$$\mathrm{TC}=\sum_{i=1}^{n}\mathrm{BW}_{U_i}c_i(x_i) \tag{4}$$

$$\mathrm{TS}=\sum_{i=1}^{n}\mathrm{BW}_{U_i}s_i(x_i) \tag{5}$$

考虑到网络中其他因素对用户行为评估所带来的干扰，在此设置干扰因子$\theta(0<\theta\leqslant1)$。由于在不同网络环境中，各网络业务用户行为的干扰是不同的，故θ的值可根据实际情况来设定，令：

$$\mathrm{TC}'=(1-\theta)\mathrm{TC} \tag{6}$$

$$\mathrm{TS}'=(1-\theta)\mathrm{TS} \tag{7}$$

当θ值越趋近于1时，意味着本次评估结果受外界的干扰程度越高，获得的结果也越不准确。

2.3 基于业务用户行为的计算机动态取证评估模型

以2.2节提出的业务用户行为评估模型为基础，引入木马技术来构建计算机动态取证模型。

2.3.1 基于木马的计算机取证

木马由于其良好的隐蔽性，使其在计算机取证方面取得了一些研究成果：文献[15]设计了一种基于木马的取证系统；文献[16]结合木马原理，设计了一种取证工具。这些成果充分考虑了木马获取证据的主动性，但没有考虑获取证据的实时性及安全性。

2.3.2 构建基于业务用户行为的动态取证评估模型

以2.2节中研究的行为评估模型为基础，研究基于业务用户行为的计算机动态取证模型(如图2)，主

要包括系统监控、取证程序植入、行为特征提取、行为评估、策略选择和证据获取模块。

1) 各模块的功能

① 系统监控模块：主要完成对系统的监控，为后续用户行为特征点的提取提供基础。

② 取证程序植入模块：对目标用户进行安全漏洞检测，根据漏洞的不同植入相应的取证程序。

③ 行为特征提取模块：采集用户行为，并保存采集信息，为后续用户行为评估提供数据支持。

④ 行为评估模块：评估用户行为是否可信(2.2中已详细介绍)，为策略选择提供依据。

⑤ 策略选择模块：以行为评估值为基础，选择相应的策略，根据策略做出不同的响应操作。

⑥ 证据获取模块：实时隐蔽地获取用户的行为，并对用户行为进行记录后发送给取证控制端。

由于篇幅限制，本文只重点讨论策略选择和证据获取模块(行为评估在2.2中已做详细介绍)。

2) 策略选择模块的设计

策略选择模块的功能是将用户行为的可信得分以及确定度值对应相应响应策略。本文将策略选择分为：不再监控、阻止操作和记录操作3种，对应的策略选择如表1所示。

表1 策略选择对应表

用户行为的评估值	用户行为的确定度值	策略的选择
高	高	不再监控
中	高	不再监控
低	高	记录操作
高	中	记录操作
中	中	记录操作
低	中	记录操作
高	低	阻止操作
中	低	阻止操作
低	低	记录操作

3) 证据获取模块的设计

以木马原理为基础进行设计，分为取证控制端和被取证端两个部分，证据获取过程如图3所示。

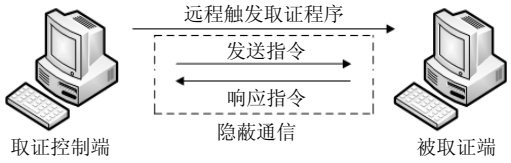

图3 证据获取过程

① 取证程序的触发：取证程序被植入目标主机以后，并不立即被激活实施取证，而是在当选择的策略为记录操作时，取证控制端才远程触发取证程序。这样可以避免取证程序被杀毒软件提前查杀，有利于保护取证程序的安全性。

② 发送指令：取证控制端在取证程序被激活后发送指令，指示取证程序实时获取指定的信息。

③ 响应指令：取证程序收到指令后对被取证端中的用户操作进行记录，再将结果返回给取证控制端；为了保证获取证据时不被发现和获取证据的安全性，在发送指令和响应指令的过程中，为了实现隐蔽通信，在仿真设计中使用Rootkit技术来实现进程和通信端口的隐藏，保证了取证控制端能实时、安全地收到被控端反馈的信息。

3 仿真实验和分析

3.1 业务用户行为评估模型的仿真实验与分析

3.1.1 实验环境与相关标准的设定

为了验证用户行为评估模型的合理性和可行性，本节构建了一个图书借阅仿真系统，主要功能包括资料下载和查询借阅信息。

假设用户登录该系统后的整体行为包含2个属性$U=\{U_1,U_2\}$，Ex_{U_1}是用户输入“用户名和密码匹配的次数”(设为m)，Ex_{U_2}是用户“超时借书的数目”的数目(设为n)；行为评价集为$C=\{C_1,C_2\}$，其中$C_1=\{$低,一般,高$\}$，$C_2=\{$多,少$\}$；同时假定用户行为属性容忍度均为5，且行为权重都相同。

规则1：当用户登录时，当$m\leqslant 2$时次时，称为匹配度高；当$2<m\leqslant 4$时，称为匹配度一般；当$m>4$时称为匹配度低；当$n\geqslant 3$时，称为超时少，否则称为超时多。

在评估标准设定后，需对评估集打分。用户行为属性集与评估标准集的对应关系如表2所示。

表2 用户行为属性集与评估集的对应关系表

用户行为属性集	评估标准集
用户名和密码匹配的次数	高匹配度
	一般匹配度
	低匹配度
超时借书的数目	超时少
	超时多
	—

规则2：每个行为的最高分数不得超过5，打分的标准就等于5减去其相应行为确定度值。

3.1.2 实验的具体步骤与结果分析

在图书借阅仿真实验中，通过调查某用户以往2000次登录的记录数据进行行为属性分析。

1) 用户行为的描述

依据表3中的数据，由逆向云发生器还原得到用

户的两个行为属性特征值分别为(1.2,0.5,0.1)，(2.5,0.2,0.1)。该用户登录系统时输入“用户名和密码匹配的次数”的云模型如图4所示。图4中的多数云滴集中在横坐标为1的左右，说明该用户在多数情况下输入1次就能匹配成功。

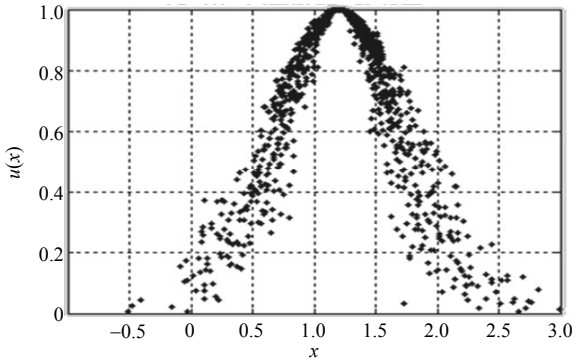

图4　表征“用户名和密码匹配的次数”的云模型图

表3　信息数据采集表

序号	U_1 用户名和密码匹配的次数	U_2 超时借书的数目
1	1	1
2	3	2
⋮	⋮	⋮
2 000	1	3

同理可得“超时借书的数目”的云模型图(略)，反映出用户“超时借书的数目”的分布情况。

2) 计算用户行为的可信得分

由表3中的数据和事先设定好的对应行为评价集和评分标准，可以得到可信得分如表4所示。

表4　用户行为评价的可信得分表

序号	C_1 用户名和密码匹配次数的可信得分	C_2 超时借书的可信得分
1	4	4
2	2	3
⋮	⋮	⋮
2 000	4	2

由表4中的数据可计算出该用户两种行为可信得分的数字特征值(3.8,0.4,0.1)和(3.5,0.3,0.2)，由此可以生成对应的云图(由于生成各行为的可信得分云模型的方法与上述生成各行为属性云模型的方法一致，故在此不再重复)。

3) 计算用户行为的可信得分

假定得到某用户的一组行为数字(2,3)，其含义是：输入用户名和密码2次成功，有3本图书超期。按照3.1.1中设定的规则，对该用户的评价为：匹配度高、超时少。根据式(2)和式(3)，计算出该用户的可信得分别为(3,2)；由式(4)和式(5)计算出该用户的最终可信得分为3。

假定该用户操作时受外界因素干扰较小(设干扰因子 θ=0.05)。排除干扰因子后，根据式(6)和式(7)计算出用户的最终可信得分为2.88。

4) 仿真实验与分析

① 首先将第一个数字2映射到表征其行为属性的云模型中，如图5所示。图5中的标识“X”指示的位置代表本次行为在“用户名和密码匹配的次数”云模型中的映射坐标，其确定度值=0.59。根据评价集和评分标准，得出可信得分=3.1，映射到云模型并修正后的可信得分=3.9，由式(3)计算出“用户名和密码匹配的次数”的可信得分 $s_1(x_1)=3.51$ 。

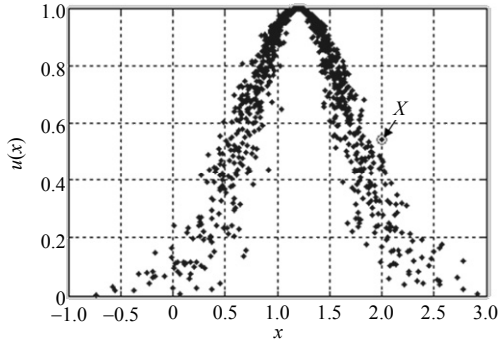

图5　“用户名和密码匹配的次数”在云模型中的映射图

② 然后将可信得分3和修正后的可信得分3.84均映射到对“用户名和密码匹配的次数”的评估云模型中，如图6所示，图6中的标识“Y”和“Z”分别代表用户行为可信得分在评估云模型中的映射，由两个点的坐标可以算出“用户名和密码匹配的次数”的行为确定度值 $c_1(x_1)=0.63$ 。

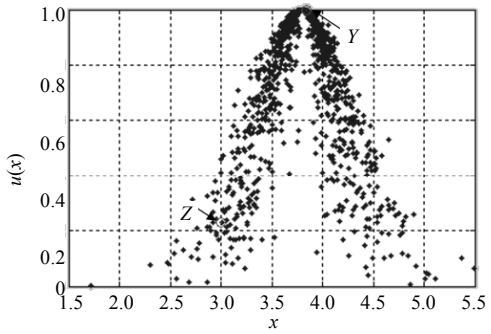

图6　“用户名和密码匹配的次数”的评估云模型图

③ 根据相同的方法，得到“超时借书”的可信得分 $s_2(x_2)=3.12$ 、确定度值 $c_2(x_2)=0.45$ 。根据式(4)和式(5)可得到用户本次整体行为可信得分=3.88，确定度值=0.62；排除网络干扰因子后，最终的可信得分=3.69，确定度值=0.59。

由图6可知，用户的实际可信得分=2.92，通过模型评估后的可信得分=3.59。实验结果有偏差的原因在于由模型得到的可信得分不仅仅只衡量用户行为的可信得分，还代表了用户行为可信的走向趋势；而对该用户行为确定度值为0.59，说明该用户继本次行为发生后，其后续行为的可信得分有59%的概率大于2.92。因此，本文模型既能对用户行为进行评估，也有预测其后续行为的能力。

3.2 计算机动态取证评估模型的仿真实现与分析

3.2.1 仿真实验与分析

本文实验以3.1节中的仿真实验为基础，实验的重点在于证据的获取。由于3.1节的实验中用户行为最终的可信得分和行为的确定度值分别为：3.59和0.59，均属于中等。对照表1可知选择策略为记录操作，将该用户的后继各种操作行为记录下来。在记录操作前需要激活取证程序，本文实验通过弹出错误提示框来激活取证程序。

取证程序对于被控端用户上网痕迹及行为文件的扫描，主要包括IE地址栏记录、IE访问历史、Cookies文件和收藏夹记录。扫描结束后将信息发送给取证控制端，取证控制端收到以后将对这些行为和文件进行分析，从中提取有用的信息。为了躲避数据监控，保证证据的安全，先对数据进行压缩，然后再传递给取证控制端，在传递过程中使用Rootkit技术实现对通信端口的隐藏。

上述实验结果充分说明了本文模型可以对用户的上网行为痕迹进行完整的记录，进一步验证了该模型的合理和可行性。

3.2.2 仿真实现与分析

基于业务用户行为的计算机动态取证仿真系统是以在前面研究的基于业务用户行为的动态取证模型的基础上，结合图书借阅系统来实现的。

1) 系统的框架结构

基于业务用户行为的计算机动态取证系统的主要模块：系统监控、行为评估和行为证据获取。

2) 仿真取证系统运行环境与工作流程

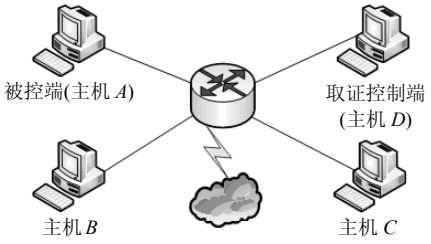

图7 仿真实现的网络拓扑结构

图7是本文仿真取证系统的网络拓扑结构图。实验中主机*A*、*B*和*C*都将访问图书借阅系统，主机*D*作为取证控制端，监控*A*、*B*和*C*发送取证指令和接收证据。工作流程为：① *A*、*B*、*C*访问用户图书借阅系统，*D*将主动获取*A*、*B*和*C*的IP地址且在其中植入取证程序，对操作进行监控，记录并提取行为数据；② 建立表征用户行为特征的云模型和与之对应的用户行为评估云模型，然后将*A*、*B*和*C*的行为分别映射到反映自身行为特征的云模型上，最终获得行为可信得分和行为确定度值；③ 根据行为的评估结果值和确定度对*A*、*B*和*C*选择不同的策略，然后根据策略进行不同的处理；④ *A*内植入的取证程序被激活，然后对*A*的各种操作行为进行记录；⑤ 取证程序将获取的信息发送给*D*；⑥ *D*接收从*A*秘密发送过来的信息。

1) 系统主要模块的实现

① 系统监控模块：借鉴了文献[15]中介绍的网页木马的相关方法，获取图书借阅系统的主机IP并在主机中植入取证程序。

② 用户行为评估模块：在实现方式上主要依靠正向云生成器算法，具体的评估方法已在3.2中详细介绍，在此不再重复。

③ 行为取证模块：包括取证程序获取被控端的信息和将获取的信息传送给取证控制端两个方面，具体方法在2.3节中已详细介绍，不再重复。

2) 系统运行结果

为体现本文系统对不同的决策所做出不同的响应结果，实验使用3个主机分别去访问图书借阅系统，对应的决策分别是不再监控、阻止操作和记录操作。当选择的决策为阻止操作时，系统就会强制其页面跳转至出错页面，从而退出该系统；当选择的策略为记录操作时，取证程序将会记录用户的各种操作。

4 结 语

业务用户行为的多样性决定了在描述和评估行为时存在的误差性和模糊性，这使得网络取证的困难度提升而准确度却降低。本文以复杂信息系统的网络环境为研究背景，借鉴已有的研究成果并引入云模型理论，提出了基于云模型理论的业务用户行为评估模型；结合木马技术，研究并提出了基于业务用户行为的计算机动态取证评估模型。通过仿真实验，进一步验证了本文研究的业务用户行为评估模型的合理性，同时还验证了计算机动态取证评估

模型能实时隐蔽的记录用户的行为，并能确保将获取的信息反馈给取证控制端。虽然目前取得了一些阶段性成果，但是针对不同业务系统的实际情况还需通过业务流进一步分析用户行为，同时有很多实际问题需要进一步研究解决。

参 考 文 献

[1] 郭树凯, 田立勤, 沈学利. FAHP在用户行为信任评价中的研究[J]. 计算机工程与应用, 2011, 47(12): 59-61.
GUO Shu-kai, TIAN Li-qin, SHEN Xue-li. Research on FAHP method in user behavior trustcomputation[J]. Computer Engineering and Application, 2011, 47(12): 59-61.

[2] 刘庆云, 张冬艳, 谭建龙, 等. 基于多维属性的网络行为控制策略[J]. 清华大学学报(自然科学版), 2013, 53(12): 1682-1687.
LIU Qing-yun, ZHANG Dong-yan, TAN Jian-long, et al. Network behavior control strategy based on multi dimension attribute[J]. Journal of Tsinghua University (Science and Technology), 2013, 53(12): 1682-1687.

[3] HALBOOB W, ABULAISH M, ALGHATHBAR K S. Quaternary privacy-levels preservation in computer forensics investigation process[C]//IEEE International Conference on Communications. [S.l.]: IEEE, 2011: 777-782.

[4] KE Hung-jui, LIU J, WANG Shiuh-jeng, et al. Hash-algorithms output for digital evidence in computer forensics[C]//IEEE International Conference on Communications. [S.l.]: IEEE, 2011: 399-404.

[5] ELEAZAR A A, MARIKO N M, HECTOR M P M. Network forensics with neurofuzzy techniques[C]//IEEE International Conference on Circuits and Systems. [S.l.]: IEEE, 2009: 848-850.

[6] HOELZ B W P, RALHA C G, GEEVERGHESE R, et al. A cooperative multi-agent approach to computer forensics [C]//IEEE International Conference on Communication. [S.l.]: IEEE, 2008: 477- 483.

[7] 戴硕, 杜晔. 一种异构分布式防火墙与入侵检测联动构架的通信机制[J]. 微电子学与计算机, 2009, 26(8): 94-97.
DAI Shuo, DU Ye. Communication mechanism design for heterogeneous distributed interaction framework between firewall and IDS[J]. Microelectronics & Computer, 2009, 26(8): 94-97.

[8] 杨卫平, 段丹青. 基于多Agent的分布式计算机动态取证模型研究[J]. 计算机应用与软件, 2008, 25(3): 81-83.
YANG Wei-ping, DUAN Dan-qing. A distributed computer dynamic forensics model based on multi-agent[J]. Computer Applications and Software, 2008, 25(3): 81-83.

[9] ZHOU Gang, MAI Yong-hao, CAO Qiang. Design and implementation of VEEL archive system for computer forensics[C]//IEEE International Conference on Communication. [S.l.]: IEEE, 2010: 138-141.

[10] 王延中. 一种基于云计算环境的动态取证模型研究[J]. 计算机测量与控制, 2012, 20(11): 3066-3069.
WANG Yan-zhong. Dynamic forensic model based on cloud computing environment[J]. Computer Measurement & Control, 2012, 20(11): 3066-3069.

[11] 张仕斌, 许春香. 基于云模型的信任评估方法研究[J]. 计算机学报, 2013, 35(2): 422-431.
ZHANG Shi-bin, XU Chun-xiang. Study on the evaluation approach based on cloud model[J]. Chinese Journal of Computers, 2013, 35(2): 422-431.

[12] WANG Dan-chen, XU Yang, PU Wei. An information system security evaluation method of business operation targeting the service composition[C]//Decision Making and Soft Computing Proceedings of the 11th International FLINS Conference. Danvers: world scientific, 2014: 589-594.

[13] ZHANG Shi-bin, XU Chun-xiang, CHANG Yan, et al. Study on trusted access model based on user behavior[J]. International Journal of Advancements in Computing Technology, 2013, 5(1): 486-495.

[14] 苗夺谦, 王国胤. 云模型与粒计算[M]. 北京: 科学出版社, 2012.
MIAO Duo-qian, WANG Guo-ying. The cloud model and granular computing[M]. Beijing: Science Press, 2012.

[15] 罗文华. 木马恶意程序电子数据取证环境的构建[J]. 警察技术, 2012, 22(2): 39-42.
LUO Wen-hua. The construction of the electronic data forensics environment of Trojan horse[J]. Police Technology, 2012, 22(2): 39-42.

[16] 吴坤鸿, 舒辉, 董卫宇. 内核脱钩技术在检测rootkit木马信息隐藏中的应用[J]. 计算机工程与设计, 2008, 19(14): 3635-3638.
WU Kun-hong, SHU Hui, DONG Wei-yu. Application of kernel decoupling technique in detection of rootkit Trojan information hiding[J]. Computer Engineering and Design, 2008, 19(14): 3635-3638.

编 辑 蒋 晓