基于隐马尔可夫模型的资源滥用行为检测方法研究

王 超[1],郭渊博[2],马建峰[1],裴庆祺[3],徐 栋[1]
(1.西安电子科技大学计算机学院,陕西西安 710071;2.解放军信息工程大学电子技术学院,河南郑州 450004;
3.西安电子科技大学计算机网络与信息安全教育部重点实验室,陕西西安 710071)

摘 要: 针对信息系统中内部人员的资源滥用行为,已有的检测方法要么不能有效检测新的资源滥用行为,要么需要获得资源滥用行为的先验知识,因而这些检测方法在应用中严重受限.本文提出了一种基于隐马尔可夫模型(HMM)的内部人员资源滥用行为检测方法.该模型以信息系统的敏感文件夹作为模型的状态,以用户的事务处理操作作为观测符号,采用Baum-Welch算法确定模型参数;基于该模型建立内部人员访问行为的HMM模型,并用于资源滥用行为检测.仿真结果表明了该检测方法的有效性.

关键词: 信息系统; 隐马尔可夫模型; 资源滥用; 内部威胁检测
中图分类号: TP309.2 **文献标识码:** A **文章编号:** 0372-2112 (2010) 06-1383-06

HMM-Based Detection Method for Resource Misuse in Information Systems

WANG Chao[1], GUO Yuan-bo[2], MA Jian-feng[1], PEI Qing-qi[2], XU Dong[1]
(1. *School of Computer Science and Technology, Xidian University, Xi'an, Shaanxi* 710071, *China*;
2. *Institute of Electronic Technology, PLA Information Engineering University, Zhengzhou, Henan* 450004, *China*;
3. *Ministry of Education Key Lab of Computer Network and Information Security, Xidian University, Xi'an, Shaanxi* 710071, *China*)

Abstract: The existing methods for resource misuse detection of information systems are restricted because of their own limitations, such as unable to detect new kinds of resource misuse and need the knowledge of potential misuses. A hidden Markov model (HMM) based method is presented to detect the resource misuse in information systems. In the HMM model, the file folders containing sensitive information are taken as the model states and the user operations as the model observation symbols. Baum-Welch algorithm is adopted to determine the model parameters. The behavioristic profiles of the insiders are determined by the HMM model and used to detect malicious behaviors. The simulation results show the effectiveness and adaptability of our method.

Key words: information system; hidden Markov model (HMM); resource misuse; insider threat detection

1 引言

美国计算机应急响应小组(CERT)[1]把恶意的内部人员(insider)定义为拥有组织的网络、系统或数据的访问权限、故意越权或者滥用访问权限以破坏组织的信息或者信息系统的安全属性的人员.恶意的内部人员熟悉系统的安全策略、安全机制和安全技术,具有系统的安全相关的知识(knowledge),因而对系统的安全性造成了极大的威胁.

内部人员的恶意行为中,资源滥用是一类主要形式[2].资源滥用是内部人员利用自己的安全凭证,违反系统的安全管理策略访问系统资源,以破坏系统的安全性.资源滥用的一个典型事例是在2007-2008年,法国兴业银行的交易员Jerome Kerviel利用合法身份进行违规交易,致使该银行巨亏71亿美元[3].另外,CERT[1]的统计资料表明,为获取经济利益而窃取/篡改雇员机密信息和窃取商业机密的事件中,合法的授权用户犯罪的比例分别高达75%和88%.由此可见,恶意内部人员的资源滥用行为发生的比例很高,造成的危害巨大.

恶意内部人员具有合法的身份和授权的访问许可,其资源滥用行为也不违反系统的安全策略和安全机制,因而难以察觉.然而,Srivastava等人[4]指出,人类的行为

收稿日期:2009-11-09;修回日期:2010-02-24;
基金项目:国家自然科学基金(No.60633020,No.60803150,No.60970143);广东联合基金重点项目(No.U0835004);陕西省自然科学基金研究计划(No.2010JQ8018);中央高校基本科研业务费专项基金

往往表现出一定的模式,在访问信息系统时也不例外.因此,研究用户信息访问系统的行为模式,发现模式之间的不一致性,将是一种可行的资源滥用行为检测方法.本文提出了一种基于隐马尔可夫模型(HMM)的资源滥用行为检测方法,主要贡献在于:(1)建立了用户行为的 HMM 模型;(2)提出了资源滥用行为的在线检测方法;(3)基于仿真数据验证了所提出的检测方法的有效性.

2 相关工作

内部人员的资源滥用行为检测研究,所采用的方法和技术多种多样,其中使用较多的是基于人工智能的方法.Lee 等人[5]提出结合实时入侵检测和数据挖掘技术,用学习代理挖掘数据、生成模式作为入侵检测的分类器,以此检测资源滥用行为.与之相似,Singhal[6]与 Ertoz 等人[7]通过挖掘入侵事件之间的关联规则非实时地检测内部人员的恶意行为.Buford 等人[8]和 Wang 等人[9]基于多代理的思想,设计了资源滥用行为的检测方法.这些研究延续入侵检测的思想,同等对待源于系统外部的攻击和内部人员的恶意行为,却忽略了攻击方法上的区别.Anderson 等人[10]采用统计学习的方法,通过评估用户当前行为与过去行为的偏离程度判断行为是否异常.Santos 等人[11]对用户的登录信息和访问过的文档进行分析,建立用户的计算模型并确定检测指标,如果分析结果与模型有偏差,则确定存在恶意的内部行为.上述基于人工智能的检测方法,大多需要标记数据训练分类器,标记数据既包含合法的用户访问行为,也包含资源滥用行为.然而在实际应用中,如何获取资源滥用行为是个难题.此外,如果标记数据不可用,则这些方法将无法检测新型的资源滥用行为.

其他的资源滥用行为检测研究中,张红斌等人[12]建立了分层映射的内部威胁模型,并用云模型描述用户行为的正常态以及偏离程度,从而实现资源滥用行为的检测.Matthew 等人[13]以 ICMAP (Information-Centric Modeler and Auditor Program)为工具周期性构建用户的 CAG (Capability Acquisition Graph),通过 CAG 搜索可能存在的内部人员攻击.在这些研究中,尽管所用方法各有不同,但是都毫无例外地以获得恶意内部用户的先验知识(如:攻击者的能力、攻击步骤、攻击成本等)为前提,只有充分掌握内部攻击者的知识,才有可能检测资源滥用行为.然而在实际应用中,在成功地检测之前获得攻击者的先验知识是个困难问题,因此这些方法的实用性难以保证.

可见,针对资源滥用行为,已有的检测方法要么无法检测新的滥用行为,要么需要先验知识,使得这些检测方法的应用受到严重限制.

对于恶意内部人员,其"内部"特性为实施攻击行为提供了便利,但也为恶意行为的检测带来了机遇—与外部攻击者相比,内部人员(可疑的内部攻击者)在人员上相对固定、数量上相对较少,这就为精确地分析和提取内部用户的行为模式提供了可能,也为成功地检测资源滥用行为提供了可能.同时,这也是资源滥用行为检测区别于入侵检测的根本所在.

文献[14]提出以应用程序相关的用户知识信息为基础,结合专业知识推导应用程序所需权限的权限控制方案,文献[15]提出基于行为特征的恶意代码识别方法,都为本文提供了很好的借鉴思路.

以"内部"特性为前提,本文提出一种内部人员的资源滥用行为检测方法:为内部人员的行为建立 HMM 模型,用正常的用户行为训练 HMM 模型并确定其模型的参数.如果内部人员的行为不能以足够高的概率被经过训练的 HMM 模型接受,则被认定是资源滥用行为.与已有的检测方法相比,采用基于 HMM 模型的检测方法的优势有:(1)无需恶意内部人员的先验知识也可进行检测;(2)HMM 模型的学习功能可减少检测误报率.

3 HMM 模型

HMM 本质上是一种统计分析模型,包含以下参数:

S:系统离散状态的集合,$S=\{s_1,s_2,\cdots,s_N\}$,势为 N;

Q:系统的状态序列,$Q=q_1,q_2,\cdots,q_X$,X 是序列中的状态数,$q_t\in S(1\leqslant t\leqslant X)$是在时刻 t 系统所处的状态;

π:初始状态概率分布,$\pi=[\pi_i]$,其中,$\pi_i=\Pr(q_1=S_i)$,且$\sum_i\pi_i=1,1\leqslant i\leqslant N$;

$\boldsymbol{A}$:状态转移矩阵,$\boldsymbol{A}=[a_{ij}]$,其中,$a_{ij}=\Pr(q_{t+1}=s_j\mid q_t=s_i)$,且$\sum_j a_{ij}=1,1\leqslant i\leqslant N,1\leqslant j\leqslant N,t=1,2,\cdots$;

O:观测符号的集合,$O=\{o_1,o_2,\cdots,o_M\}$,势为 M;

$\boldsymbol{B}$:观测符号矩阵,$\boldsymbol{B}=[b_{jk}]$,其中,$b_{jk}=\Pr(o_k\mid s_j)$,且$\sum_k b_{jk}=1,1\leqslant j\leqslant N,1\leqslant k\leqslant M$;

P:观测符号序列,$P=p_1,p_2,\cdots,p_Y$,Y 是序列中的观测符号数,$p_t\in O(1\leqslant t\leqslant Y)$是在时刻 t 系统的观测符号.

HMM 是一个双重的随机过程,由两部分组成:马尔可夫链和一般随机过程(见图 1).其中,马尔可夫链描述系统的状态转移,受状态转移矩阵 $\boldsymbol{A}$ 控制,初始状态概率分布为 π;一般随机过程描述系统的状态与观测符号之间的统计关系,受观测符号矩阵 $\boldsymbol{B}$ 控制.HMM 模型中,状态及其转移过程不可观测,外界只能通过观测符号序列去推测.

清楚地描述 HMM 模型需要确定 π、$\boldsymbol{A}$、$\boldsymbol{B}$(包括 N 和 M)等参数,HMM 模型用 $\lambda=(\boldsymbol{A},\boldsymbol{B},\pi)$表示.

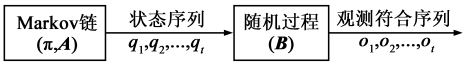


图1　HMM示意图

系统的观测符号序列 P 可能来自于系统的多个状态序列,考虑相同长度的系统状态序列和观测符号序列

$$\begin{cases} Q = q_1, q_2, \cdots, q_R \\ P = p_1, p_2, \cdots, p_R \end{cases}, \tag{1}$$

由序列 Q 生成序列 P 的概率是:

$$\Pr(P \mid Q, \lambda) = \prod_{t=1}^{R} \Pr(P_t \mid q_t, \lambda), \tag{2}$$

如果观测符号的出现是相互独立的,式(2)可以展开成:

$$\Pr(P \mid Q, \lambda) = b_{q_1}(O_1) b_{q_2}(O_2) \cdots b_{q_R}(O_R), \tag{3}$$

状态序列 Q 出现的概率是:

$$\Pr(Q \mid \lambda) = \pi_{q_1} a_{q_1 q_2} a_{q_2 q_3} \cdots a_{q_{R-1} q_R} \tag{4}$$

因此,用参数 λ 表示的 HMM 生成观测符号序列 P 的概率是:

$$\Pr(P \mid \lambda) = \sum_{Q} \Pr(P \mid Q, \lambda) \Pr(Q \mid \lambda) \tag{5}$$

HMM 模型可解决的一类基本问题是对于给定的观测符号序列,预测新的观测符号序列出现的概率.在信息安全领域中,攻击者的先验知识难以获得,导致其特征难以提取,而用户的行为相对易于监控.因此,以用户的行为作为 HMM 模型的观测符号,连续收集用户的操作并建立用户的行为模式,通过预测可能出现的用户行为可实现异常行为检测.而且,持续收集用户的操作可实现行为模式的进化,可减少误报率和新型恶意行为的漏报率.近来,HMM 模型及其扩展形式在信息安全领域已有应用[4,16].本文将基于 HMM 模型开发内部人员的资源滥用行为检测方法.

4　基于 HMM 的资源滥用检测方法

不失一般性,我们将以基于 Windows 操作系统的信息系统为例说明本文设计的资源滥用行为检测方法.

假设在一个信息系统中保存了一些敏感文件,这些文件集中分布在系统内的若干个敏感文件夹中,用户在这些文件夹中完成敏感信息的事务处理操作.事务处理操作有读取文件(r)、写入文件(w)、复制文件(c)、删除文件(d)、移动文件(m)和打开/创建文件(o).其中,进程读取和写入等多个操作都需要调用打开/创建文件函数,而且打开/创建文件操作一般不会破坏信息系统的安全性,所以本文忽略打开/创建文件操作.

我们收集内部人员的行为信息,采用应用程序接口挂接(API hook)技术截取用户进程对文件操作函数的调用,当用户进程调用相关函数时判断目的文件路径.涉及敏感文件夹的操作都将被记录,形成该内部人员的操作序列.在监视用户行为的过程中,只记录用户的操作,而操作的对象和操作值都被忽略.例如:内部人员 A 对敏感文件夹 B 中的文件 C 执行了"写入"操作,监视系统只记录 A 的"写入"行为,而忽略文件夹 B、文件 C 以及写入的内容.这种监视方法既可以获取用户的操作序列,又不涉及信息系统的敏感信息和用户隐私,因此,不会增加信息系统的安全隐患.

4.1　内部人员行为的 HMM 模型

在收集内部人员行为信息的过程中,可观测到的是用户的事务处理操作序列,而操作的对象和操作值是不可见的.由此,建立内部人员行为的 HMM 模型(见图 2).

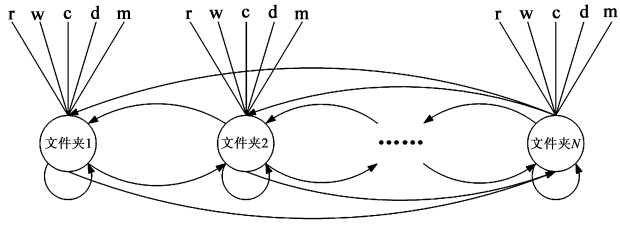


图2　用户行为的HMM模型

HMM 模型中,状态是保存敏感信息的文件夹,观测符号是用户在各个文件夹上执行的操作.一个用户在系统内的敏感文件夹中执行事务处理操作,其行为造成 HMM 模型的状态转移,其表现是监视系统截取的用户操作序列.如果系统中需要保护的文件数量较少,可以以敏感文件作为 HMM 模型的状态,观测符号也是用户的操作,建立的 HMM 模型和检测方法大体相同.因此,本文中仍以敏感文件夹作为 HMM 模型的状态.

4.2　HMM 模型的参数建立

建立用户行为的 HMM 模型,最重要的是确定模型的参数 $\boldsymbol{A}$、$\boldsymbol{B}$ 和 π.在本文的用户行为建模过程中,已知的模型参数是 N、M,需要通过截取的观测符号序列和设定的模型参数初值确定模型参数 $\boldsymbol{A}$、$\boldsymbol{B}$ 和 π.为简单起见,$\boldsymbol{A}$、$\boldsymbol{B}$ 和 π 的初值都设为均匀分布,即:HMM 模型以任意状态作为初始状态的概率都是 $1/N$,模型中状态之间的一步转移概率也是 $1/N$,在每个状态任意观测符号出现的概率是 $1/M$.以 N、M 和 $\boldsymbol{A}$、$\boldsymbol{B}$、π 的初值为基础,采用 Baum-Welch 算法[17]训练 HMM 模型,确定模型参数.

训练 HMM 模型需要基于正常的用户行为.然而在实际的信息系统中,相比正常的用户行为,资源滥用行为只是极少数.HMM 模型本质上是统计分析模型,因此,以截取的用户操作序列作为 HMM 模型的训练数据即可.

4.3　资源滥用行为的检测方法

HMM 模型经过训练后,模型参数 $\boldsymbol{A}$、$\boldsymbol{B}$ 和 π 都被确

定下来,用 $\lambda=(\boldsymbol{A},\boldsymbol{B},\pi)$表示这个 HMM 模型.

对于 HMM 模型 λ,到时刻 t 输出长度为 R 的观测符号序列 $P_1=o_1,o_2,\cdots,o_R$,该序列出现的概率 p_1 是:

$$p_1=\Pr(P_1|\lambda)=\Pr(o_1,o_2,\cdots,o_R|\lambda). \tag{6}$$

在 $t+1$ 时刻,HMM 模型输出观测符号 o_{R+1},丢弃 o_1 后得到一个新的长度为 R 的观测符号序列 $P_2=o_2,\cdots,o_R,o_{R+1}$,该序列出现的概率 p_2 是:

$$p_2=\Pr(P_2|\lambda)=\Pr(o_2,\cdots,o_R,o_{R+1}|\lambda) \tag{7}$$

计算这两个序列出现概率的差值 Δp:

$$\Delta p=p_1-p_2. \tag{8}$$

如果 $\Delta p\leqslant 0$,说明对于经过训练的 HMM 模型来说,新观测符号序列出现的概率在增加,观测符号 o_{R+1}是正常行为;而 $\Delta p>0$ 说明 P_2 出现的概率比 P_1 出现的概率小,所以新序列被 HMM 模型接受的概率低,o_{R+1} 可能是一次资源滥用行为.依照信息系统的安全需求设定阈值 th,如果有:

$$\Delta p/p_1\geqslant th, \tag{9}$$

判定 o_{R+1}是资源滥用行为.

o_{R+1}被判定为异常行为,则监视系统立即报警;否则 o_{R+1}加入观测符号序列,作为检测下一个观测符号的基础序列.随着时间的推移,用户的行为模式可能会发生改变.不断在观测符号序列中添加新到达的观测符号,其意义在于连续学习用户的行为模式,降低监视系统的误报率.

HMM 模型的训练和资源滥用行为的检测方法如图 3 所示.

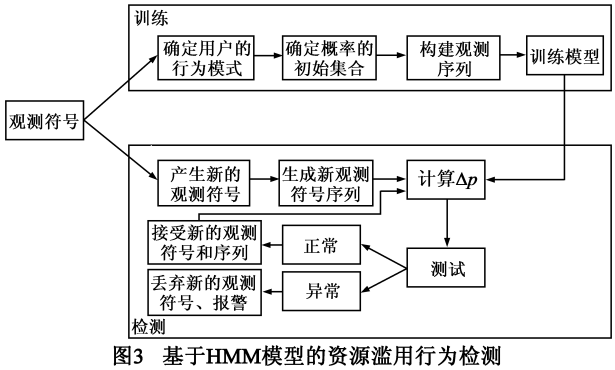


图3 基于HMM模型的资源滥用行为检测

5 实验结果与分析

异常行为的检测结果可分为四种:漏报(FN)、误报(FP)、命中(TP)、正常(TN).本文将以 Stolfo 等人[18]提出的"TP-FP"和准确率(accuracy)作为检测方法的评价指标.

5.1 模型参数的确定

本文将在 Matlab7.0 上采用仿真实验的方法验证我们设计的资源滥用行为检测方法的有效性.

实验的参数设定:假设信息系统中有 4 个敏感文件夹,$N=4$;在这些文件夹上的操作类型有 5 种(读取、写入、删除、复制和移动),$M=5$;内部人员的行为统计特性可通过监视系统取得,假设某内部人员的行为统计特性为:44% 读取操作、35% 写入操作、7% 复制操作、3% 删除操作和 11% 移动操作;建立该用户行为模式的 HMM 模型,其观测符号序列按其行为特性完全随机生成.设观测符号序列的长度为 R,判别阈值为 th.

实验中,按照设定的用户行为统计特性,随机生成 25 组、每组 33 个符号的观测符号序列,采用 Baum-Welch 算法训练 HMM 模型.选择 25 组训练数据既可避免计算量过大的问题,又能保证完成训练过程.每组选择 33 个观测符号,可从概率上保证每个观测符号都将会出现;实验中发现,训练完成时,$\boldsymbol{A}$、$\boldsymbol{B}$ 和 π 取值如下:

$$\boldsymbol{A}=\begin{Bmatrix}0.17528 & 0.24386 & 0.08542 & 0.49544\\ 0.21340 & 0.30511 & 0.29359 & 0.18790\\ 0.04599 & 0.47467 & 0.09133 & 0.38801\\ 0.04833 & 0.37025 & 0.57069 & 0.01073\end{Bmatrix} \tag{10}$$

与 $\boldsymbol{A}$ 相对应的 $\boldsymbol{B}(r,w,c,d,m)$和 π 为:

$$\boldsymbol{B}=\begin{Bmatrix}0.13316 & 0.54786 & 0.02870 & 0.00890 & 0.28138\\ 0.47061 & 0.44805 & 0.02029 & 0.01419 & 0.04686\\ 0.26437 & 0.33615 & 0.13021 & 0.01886 & 0.25041\\ 0.74345 & 0.14879 & 0.09897 & 0.00812 & 0.00067\end{Bmatrix} \tag{11}$$

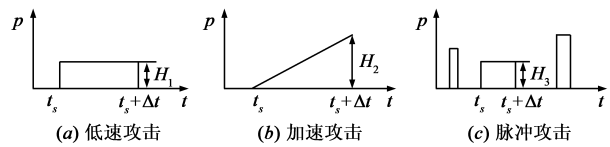
$$\pi=(0.22291\quad 0.26358\quad 0.19615\quad 0.31736). \tag{14}$$

根据随后多次实验的结果,观测序列的长度 R 在[5,13]上取值、阈值 th 在[0.1,0.5]上取值可取得较好的检测结果.

5.2 仿真实验

在本文的实验中,我们用替换观测符号的方法模拟资源滥用行为,即用随机生成的观测符号替换序列中的观测符号,并保证替换前后的相应位置上的观测符号绝不相同.

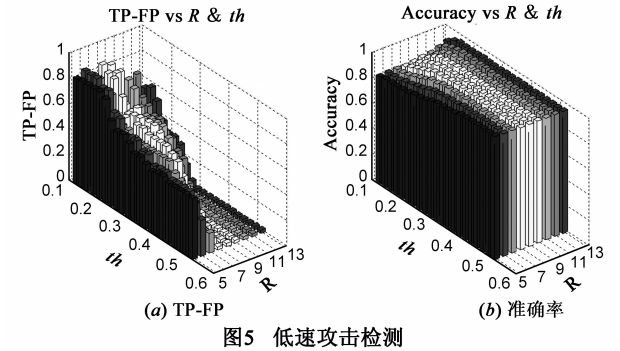
在此,考虑三种不同表现形式的内部人员资源滥用行为:(1)低速攻击:在很长的一段时间内,发生的频率低而稳定;(2)加速攻击:在一段时间内,发生的频率逐渐加快;(3)脉冲攻击:发生的时间和强度均不稳定,具有冲击特性.这三种形式的资源滥用行为分别如图 4 (*a*)、(*b*)和(*c*)所示.在实际应用中,这三种形式的攻击具有很强的代表性.



(*a*) 低速攻击 (*b*) 加速攻击 (*c*) 脉冲攻击

图4 不同表现形式的资源滥用行为

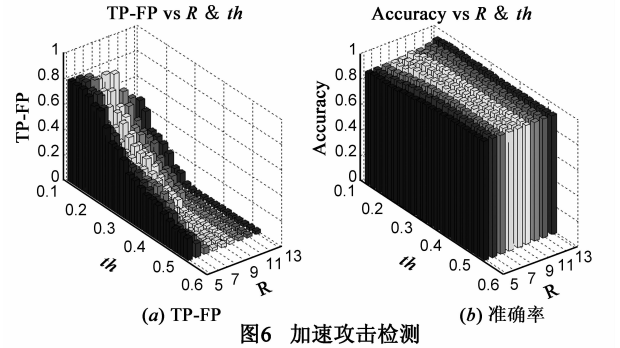
对于第一种形式的资源滥用行为,我们在训练数据的每个分组中,分别随机替换 1 个观测符号.本文检测方法的 TP-FP 和准确率如图 5(*a*)和(*b*)所示.



(*a*) TP-FP　　(*b*) 准确率

图5　低速攻击检测

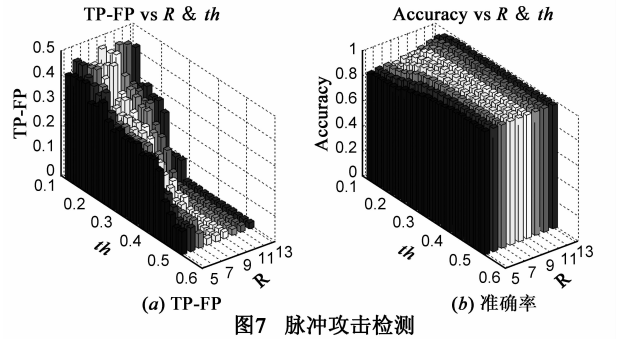
对于第二种形式的资源滥用行为,我们在训练数据的第 1 ~ 5 分组中,每个分组中随机替换 1 个观测符号;在第 6 ~ 10 分组中,每个分组随机替换 2 个观测符号,依此类推.本文检测方法的 TP-FP 和准确率如图 6(*a*)和(*b*)所示.



(*a*) TP-FP　　(*b*) 准确率

图6　加速攻击检测

对于第三种形式的资源滥用行为,我们在总长 825 的观测符号序列中,随机选择六处进行替换.替换过程中,用于替换的符号序列长度在 3 ~ 6 之间随机选择,已经被替换的符号不会被再次替换.本文检测方法的 TP-FP 和准确率如图 7(*a*)和(*b*)所示.



(*a*) TP-FP　　(*b*) 准确率

图7　脉冲攻击检测

从实验结果看,TP-FP 和准确率都随着 R 和 th 的增加,呈现先增加后减小的趋势.对于 TP-FP,其最大值的三维坐标分别是(8,0.12,0.8),(7,0.12,0.78) 和(7,0.16,0.45).所以在检测过程中,取 $R_{o1}=8$、$th_{o1}=0.14$,TP-FP 可取得最大值.对于准确率,其最大值的三维坐标分别是(8,0.26,0.97),(8,0.22,0.93),(9,0.24,0.96).所以在检测过程中,取 $R_{o2}=8$、$th_{o2}=0.24$,准确率可能取得最大值.

在 R 和 th 值较小时,TP-FP 较为接近峰值,随着 R 和 th 值的增加,TP-FP 快速回落.所以,对于 TP-FP 指标较为重要的场合,R 和 th 值宜取值偏小.在 R 和 th 值较小时,准确率迅速增加接近峰值,随后趋于稳定.所以取较大的 R 和 th 值,可保证检测方法的准确性.

本文的实验以最具代表性的三种资源滥用行为为研究对象,研究了资源滥用行为检测方法的性能.本文的检测算法总体上表现出很高的准确率,分别为 84% ~ 97%、86% ~ 93% 和 83% ~ 96%.这个结果表明,对于不同形式的资源滥用行为,本文的检测方法具有很好的适应性.

6　结论

对于不同来源的异常行为,其检测方法存在本质差异.本文从内部人员的"内部"特性出发,提出了一种基于 HMM 模型的内部人员资源滥用行为检测方法.在该模型中,信息系统的敏感文件夹作为模型的状态,用户在文件夹上的操作行为作为观测符号,采用 Baum-Welch 算法确定模型参数.我们提出了内部人员行为的建模方法,用于资源滥用行为的检测.仿真结果表明,该检测方法对常见的攻击形式有很好的检测率和适应性.

参考文献:

[1] D Cappelli, A Moore, R Trzeciak, et al. Common Sense Guide to Prevention and Detection of Insider Threats-Version 3.1 [R]. Carnegie Mellon University, 2009.

[2] S StolfoJ, S Bellovin, S Hershkop, et al. Insider Attack and Cyber Security: Beyond the Hacker[M]. New York: Springer Science + Business Media, 2008. 70 – 71.

[3] G Viscusi, A Chassany. Societe Generale Reports EU4.9 Billion Trading Loss [DB/OL]. http://www.bloomberg.com/apps/news? pid = 20601087&sid = azUPx3TKR8zs, 2008.

[4] A Srivastava, A Kundu, S Sural, et al. Credit card fraud detection using hidden markov model[J]. IEEE Transactions on Dependable and Secure Computing, 2008, 5(1): 37 – 48.

[5] W Lee, S Stolfo, P Chan, et al. Real time data mining-based intrusion detection [A]. Proceedings of the 2001 DARPA Information Survivability Conference and Exposition II[C]. Wisconsin: World Scientific and Engineering Academy and Society (WSEAS), 2001. 89 – 100.

[6] A Singhal. Data Warehousing and Data Mining Techniques for Computer Security [M]. New York: Springer-Verlag, 2006. 83

– 103.
[7] L Ertoz, E Eilertson, A Lazarevic, et al. MINDS-Minnesota intrusion detection system [A]. Kargupta H, Joshi A, Sivakumar K, et al. Next Generation Data Mining [M]. New York: MIT/AAAI Press, 2004. 65 – 86.
[8] J Buford, L Lewis, G Jakobson. Insider threat detection using situation-aware MAS [A]. Proceedings of the 11th International Conference on Information Fusion [C]. New York: IEEE Press, 2008. 1 – 8.
[9] H Wang, S Liu, X Zhang. A prediction model of insider threat based on multi-agent [A]. Proceedings of the 1st International Symposium on Pervasive Computing and Applications[C]. New York: IEEE Press, 2006. 273 – 278.
[10] D Anderson, T Lunt, H Javitz, et al. Detecting Unusual Program Behavior Using the Statistical Component of the Next-Generation Intrusion Detection Expert System (NIDES)[R]. Technical Report SRI-CSL-95-06, SRI International, 1995.
[11] E Santos, H Nguyen, F Yu, et al. Intent-driven insider threat detection in intelligence analyses [A]. Proceedings of the 2008 IEEE/WIC/ACM International Conference on Web Intelligence and Intelligent Agent Technology [C]. New York: IEEE Press, 2008. 345 – 349.
[12] 张红斌,裴庆祺,马建峰. 内部威胁云模型感知算法[J]. 计算机学报, 2009, 32(4): 784 – 792.
ZHANG Hong-Bin, PEI Qing-Qi, MA Jian-Feng. An algorithm for sensing insider threat based on cloud model[J]. Chinese Journal of Computers, 2009, 32(4): 784 – 792. (in Chinese)
[13] S Matthew, S Upadhyaya, D Ha, et al. Insider abuse comprehension through capability acquisition graphs[A]. Proceedings of the 11th International Conference on Information Fusion [C]. New York: IEEE Press, 2008. 9 – 16.
[14] 姚立红,訾小超,茅兵 等. 针对权限滥用的安全增强研究[J]. 电子学报, 2003, 31(11): 1747 – 1749.
YAO Li-hong, ZI Xiao-chao, MAO Bing, et al. Research on security enhancement to privilege abuse[J]. Acta Electronica Sinica, 2003, 31(11): 1747 – 1749. (in Chinese)
[15] 刘巍伟,石勇,郭煜. 一种基于综合行为特征的恶意代码识别方法[J]. 电子学报, 2009, 37(4): 696 – 700.
LIU Wei-wei, SHI Yong, GUO Yu, et al. A malicious code detection method based on integrated behavior characterization [J]. Acta Electronica Sinica, 2009, 37(4): 696 – 700. (in Chinese)
[16] Y Xie, S Yu. A large-scale hidden semi-Markov model for anomaly detection on user browsing behaviors [J]. IEEE/ACM Transactions on Networking, 2009, 17(1): 54 – 65.
[17] L Rabiner. A tutorial on hidden markov models and selected applications in speech recognition [J]. Proceedings of the IEEE, 1989, 77: 257 – 286.
[18] S Stolfo, D Fan, W Lee, et al. Cost-based modeling for fraud and intrusion detection: Results from the JAM project [A]. Proceedings of the DARPA Information Survivability Conference and Exposition[C]. Wisconsin: World Scientific and Engineering Academy and Society (WSEAS), 2000. 130 – 144.

作者简介:

王 超 男,1976 年生,博士,讲师,主要研究领域为网络系统的安全性与可生存性.
E-mail: xdkevin@gmail.com

郭渊博 男,1975 年生,博士,副教授,主要研究领域为无线网络安全与系统可生存性.
E-mail: yuanbo_g@hotmail.com

马建峰 男,1963 年生,教授,博导. 主要研究领域为计算机安全、密码学、移动与无线网络安全. E-mail: jfma@mail.xidian.edu.cn.

裴庆祺 男,1975 年生,博士,副教授,中国电子设备系统工程公司研究所博士后,主要研究领域为系统安全防护、无线网络及其安全、数字版权管理等. E-mail: qqpei@xidian.edu.cn.

徐 栋 男,1988 年生于江苏镇江,学士,主要研究领域为信息安全防护. E-mail: xudong.whrl@163.com.