基于行为序列灰色模糊判定的计算机木马检测方法

胡光俊[1,2]， 宋伟航[2]， 徐国爱[1]
(1. 北京邮电大学 网络与信息攻防技术教育部重点实验室，北京 100876；2. 公安部第一研究所，北京 100048)

摘 要：针对计算机木马判定困难的问题，提出了一种对行为序列进行多属性灰色模糊木马判定的方法. 通过对计算机木马定性分析构建了木马攻击树，归纳了木马使用攻击树叶子节点方法实现不同功能的概率等级. 使用基于木马行为的检测技术检测出主机包含网络通信、隐蔽运行、开机启动、自我防护四要素的所有行为序列，视这些行为序列为木马设计方案，使用模糊数量化定性指标，将灰色系统理论与模糊优选结合，计算各方案的木马灰色模糊的优属度，最后使用危险指数进行木马判定. 应用示例表明该方法可以有效区分正常程序，检出木马程序.

关键词：木马检测；木马攻击树；行为序列；模糊数；灰色模糊优属度
中图分类号：TP 393.08 **文献标志码**：A **文章编号**：1001-0645(2011)05-0567-05

Behavior Sequence Based Grey Fuzzy Determinant for Computer Trojan Detection

HU Guang-jun[1,2]， SONG Wei-hang[2]， XU Guo-ai[1]
(1. Key Laboratory of Network and Information Attack & Defence Technology, Minstry of Education of China, Beijing University of Posts and Telecommunications, Beijing 100876, China; 2. The First Research Institute of Ministry of Public Security, Beijing 100048, China)

Abstract: A multiple attribute grey fuzzy Trojan detecting method based on behavior sequence is proposed to solve the problems of Trojan detection. Through qualitative analysis, Trojan attack tree was constructed. The probability level, that Trojan can complete different functions by the method of using leaves node of attack tree, was summed up. Behavior sequences of Trojan, including network communication, hidden running, starting up after power on and self-protection, were considered as the designing scheme of Trojan. Then, by the combination of grey system theory and fuzzy optimization method, the grey fuzzy optimal degree for each Trojan scheme can be calculated with the use of quantized qualitative index of fuzzy number. At last, Trojan was detected by comparing grey fuzzy optimal degree with the dangerous index. The example shows that above method can effectively distinguish the Trojan from normal program.

Key words: Trojan detection; Trojan attack tree; action sequence; fuzzy number; grey fuzzy optimal degree

对木马的检测和判定一般分为静态和动态两类. 静态检测指对木马程序进行静态特征分析提取，然后对程序使用判定规则进行推理判定. 如特征码匹配法[1]，通过静态分析PE文件，获取程序运行时可能调用的API集合，将其和木马攻击常用的API调用序列作匹配，最后用静态危险指数来判定.

动态检测指监控系统的资源条件，将程序在安装、启动、运行中的动作与木马动作匹配后进行判定. 如检测注册表/系统文件法[2]，根据Windows操作系统下，写注册表、修改系统启动脚本文件、注

收稿日期：2010-09-22
基金项目：国家"八六三"计划项目(2009AA01Z439)
作者简介：胡光俊(1979—)，男，在职博士生，工程师，E-mail：cityof93@bupt.edu.cn.

入系统文件是木马隐蔽启动的主要方式，通过监视检测注册表项和系统文件状态判定木马；线程-端口关联法[3]，根据木马服务端通常要与控制端进行网络通信，通过直接扫描系统的活动线程以及截拦活动线程的网络数据流量来进行木马检测和判定；系统挂钩(HOOK)检测法[4]，根据现代木马常常采用Rootkit技术进行隐蔽以便逃避查杀，在分析用户进程空间与内核空间中系统函数调用标志信息的基础上，检测系统中是否存在挂钩(HOOK)从而进行木马判定；虚拟机检测法[5]，通过仿真CPU(如X86)，用解释的方法执行程序并监测可疑行为进行木马判定，如Symantec的Bloodhound技术和McAfee的Advanced Heuristics技术.

木马检测方法虽然众多，但在文献[6]中描述了实验木马使用系统服务描述表(SDT)恢复方法躲避的植入/运行时的行为检测，使用传输驱动程序接口(TDI)/网络驱动程序接口(NDIS)恢复方法躲避通信时的行为检测，从而对卡巴斯基免杀. 以上情况说明单一木马检测方法无法解决漏报与误报问题. 因此，作者提出使用动态检测方法获得可疑行为序列，通过计算各个行为序列的木马灰色模糊的优属度，最终使用危险指数判定木马的新方法.

1 木马攻击树

1.1 攻击树概念

B. Schneier[7]基于软件故障树方法提出攻击树模型. 在一棵攻击树的树形结构中，根节点表示总目标，非叶节点表示攻击的各子目标，节点表示达到上级节点目标的方法，各个分支表示达到总目标的方法. 节点之间的关系是“与”，“或”，如图1所示.

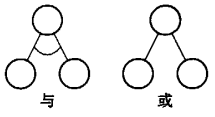

图1 攻击树的“与”“或”

Fig. 1 Attack tree's logic “and” and “or”

“与”关系表示所有子结点目标完成才可以导致父结点目标的完成，“或”关系表示任一子结点目标的完成都可以导致父结点目标完成. 攻击树的节点根据需要可以赋予多种类型的参数值，例如攻击能否实现的布尔值、攻击的成本等.

1.2 木马攻击树

木马程序攻击的最终目标是控制主机，窃取计算机资源，为达到这一目标需要完成一系列二级目标，包括：隐蔽植入，开机启动，隐蔽运行，网络连接，自我防护. 基于攻击树模型，结合木马攻击特点进行以下定义.

定义1 木马攻击树(Trojan attack tree)由3元组$\{N,S,V\}$组成，其中N为以树节点为元素的非空有限集合，每个非叶节点代表攻击目标，叶节点代表攻击方法；S为节点的状态非空有限集合，为布尔类型，为真则表示木马完成了节点代表的目标或使用了节点代表的攻击方法；V为在木马检测过程中，判断检测到的叶子节点方法是木马发起的可能性修订本，分为5级：基本不可能、不太可能、可能、很可能、极可能.

按照定义1构建木马攻击树如图2所示.

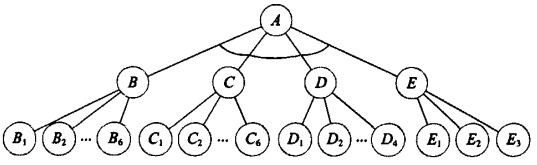

图2 木马攻击树

Fig. 2 Trojan attack tree

节点具体含义及V如表1所示.

表1 攻击树节点含义及V

Tab. 1 Meaning of attack tree nodes and V

节点	含义	V
A	窃取计算机资源	
B	网络通信	
C	隐蔽运行	
D	开机启动	
E	自我防护	
B_1	端口复用	极可能
B_2	基于域名的端口反弹	可能
B_3	发送数据远大于接收	很可能
B_4	高级协议连接	可能
C_1	磁盘文件搜索读写	可能
C_2	用户键盘记录	极可能
C_3	用户屏幕截屏	极可能
C_4	发起大量连接	极可能
C_5	嗅探网络数据	极可能
D_1	修改注册表启动项	可能
D_2	修改开机启动脚本	可能
D_3	开机启动文件劫持	极可能
D_4	注册系统服务	可能
D_5	根目录Autorun	很可能
D_6	修改开机启动目录	不太可能
E_1	无图标无窗口进程	很可能
E_2	远程线程注入	很可能
E_3	动态链接库劫持	很可能
E_4	程序文件在系统目录	可能
E_5	文件/模块/连接隐藏	极可能
E_6	通信内容隐藏	可能

2　木马行为序列

2.1　基于行为的木马检测

基于行为的木马检测是将一系列已经规定好的异常行为作为规则,通过监视系统运行程序的行为结合规则来判定程序是否为木马.

木马行为分析技术可以划分为基于主机资源访问行为、基于主机系统调度行为和基于网络行为分析 3 类. 基于主机资源访问行为指木马程序对文件、目录、注册表、键盘、鼠标、屏幕等操作,这些操作常在木马进行开机启动和隐蔽运行时发起;基于主机系统调度行为指木马对运行中系统的进程、线程、加载的模块、系统函数等的操作,这些操作常在木马隐蔽允许和自我防护时使用;基于网络行为指木马使用 TCP/UDP/ICMP/HTTP/DNS 等协议发起打开端口、端口复用、域名解析、建立连接、传输数据等操作,这些操作在木马网络通信中使用.

使用主机资源访问行为、主机系统调度行为和网络行为检测技术可以实现对木马攻击树叶子节点方法的全部检测.

2.2　基于行为序列的木马检测

定义 2　行为序列(action sequence)是针对一个事件,按照顺序组织的行为的集合,是一个多元组 $(B_1,B_2,\cdots,B_n)$. 对于木马检测事件,按照以下顺序组织行为序列:网络通信检测→隐蔽运行检测→开机启动检测→自我防护检测.

基于行为分析的木马检测方法难点在于异常行为的界定. 随着恶意代码实现技术特别是隐藏技术的不断发展,随着 P2P 技术和自动升级应用的大规模出现,使得木马与正常应用程序之间的界限越来越模糊,单一角度的行为检测已经不能解决问题. 但从行为序列的整体角度看,木马与正常程序还是存在显著差异的,通过将可疑行为序列与木马行为序列进行比较判定能稳定提高木马检测的检出率.

3　多属性灰色模糊判定方法

视使用行为检测方法得到的多个可疑程序的行为序列为木马设计方案,视实现网络通信、隐蔽运行、开机启动、自我防护二级目标使用方法可能被木马使用的概率为方案评价指标,将木马判定问题转换为多属性木马方案决策问题. 由于 4 个指标都是定性指标,首先使用模糊数对指标进行量化,然后使用基于灰色关联分析的模糊优选模型对木马方案进行排序,最后使用危险指数进行木马判定.

3.1　评价指标量化

不同方法被木马程序用来实现网络通信、隐蔽运行、开机启动、自我防护功能的概率不同,在评价是否是木马行为时常使用"很可能"、"可能"、"不太可能"等评语定性描述,这些评语可以使用梯形模糊数[8]进行量化.

定义 3　评语集(comment)$V=\{\omega_1,\omega_2,\cdots,\omega_m\}$,是对使用叶子节点方法实现二级目标概率的评价结果的集合. 针对木马攻击树模型的木马行为评语集,取 $m=5$,梯形模糊数表示如表 2 所示.

表 2　评语梯形模糊数

Tab. 2　Trapezoidal fuzzy number of comment

评语	序号	梯形模糊数
不可能	ω_1	(0,0;0,0.2)
不太可能	ω_2	(0,0.2;0,0.2)
可能	ω_3	(0.5,0.5;0.2,0.2)
很可能	ω_4	(0.8,1.0;0.2,0)
极可能	ω_5	(1.0,1.0;0.2,0)

相应的隶属函数如图 3 所示.

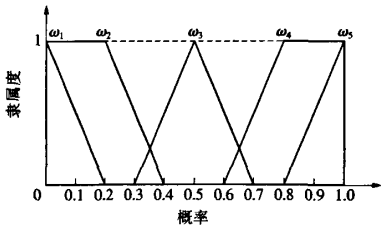

图 3　评语模糊数隶属度函数图

Fig. 3　Membership function of comment fuzzy number

定义 4　行为序列评语(action sequence comment)$\boldsymbol{A}$ 包括网络通信评语,隐蔽运行评语,开机启动评语,自我防护评语,即

$$\boldsymbol{A}=[V_1\quad V_2\quad V_3\quad V_4].$$

行为序列评语是定性评价的量化结果,取值为下级叶子节点中 S 为真的叶子节点 V 大者.

3.2　方案属性指标的规范化

3.2.1　确定理想方案指标序列

1 个木马设计方案 T_i 是 4 个属性指标的映射,即 $T_i=f_i(V_1,V_2,V_3,V_4)$.

方案排序过程实质是比较属性指标的优劣,备选方案 i 所具有的属性指标就构成了进行灰色关联分析的比较序列向量 $\boldsymbol{A}_i=[V_{i1}\quad V_{i2}\quad V_{i3}\quad V_{i4}]$.

对方案进行比较,必须构建 1 个参照序列 $\boldsymbol{A}_0$. 由于方案优选具有比较上的相对性,可以定义 1 个

假想的理想方案，该方案的各属性指标均为最优值，即表征理想方案的指标序列为

$$\boldsymbol{A}_0=[V_{01}\quad V_{02}\quad V_{03}\quad V_{04}]=[\omega_5\quad \omega_5\quad \omega_5\quad \omega_5]. \tag{1}$$

3.2.2 模糊数规范化

进行评判时需要消除量纲的影响并统一度量尺度，即对属性指标进行规范化处理，以保证评判的等效性. 其规范化公式为

$$V_{ij}^0=\begin{cases}V_{ij}/V_{0j} & \text{指标越大越优}\\ V_{0j}/V_{ij} & \text{指标越小越优}\end{cases}, \tag{2}$$

它表示的是属性指标相对于理想指标的接近度，由此形成规范的理想参照序列 $\boldsymbol{A}_0^0=[1\quad 1\quad 1\quad 1]$ 和比较序列 $\boldsymbol{A}_i^0=[V_{i1}^0\quad V_{i2}^0\quad V_{i3}^0\quad V_{i4}^0]$.

依据式(2)，要对模糊数进行规范化，需首先解决模糊数除运算问题和解模糊问题. 设2个梯形模糊数 $M=(a,b;\alpha,\beta)$ 和 $N=(c,d;\gamma,\delta)$，依据Bonissone研究成果得到模糊数除运算近似公式[9]为

$$M/N\approx[a/d,b/c;(a\delta+d\alpha)/d(d+\delta),\ (b\gamma+c\beta)/c(c-\gamma)]. \tag{3}$$

用式(5)对定性指标进行规范化处理后，利用模糊数的整体期望值对定性指标的规范结果进行解模糊[8]得到规范化解模糊决策矩阵. 对于梯形模糊数 $\widetilde{A}=(m,n;\alpha,\beta)$，其整体期望值为

$$I(\widetilde{A})=(2m+2n+\beta-\alpha)/4. \tag{4}$$

3.3 灰色模糊的优属度

3.3.1 方案的灰色模糊隶属度

对方案的比较序列和理想参照序列进行关联分析，得到方案指标相对其理想值的灰色隶属度[10]为

$$\gamma_{ij}=\frac{\Delta_{\min}+\zeta\Delta_{\max}}{\Delta_{ij}+\zeta\Delta_{\max}}. \tag{5}$$

式中：

$$\Delta_{\min}=\min_{i\in m}\min_{i\in m}|x_{0j}-x_{ij}|,$$

$$\Delta_{\max}=\max_{i\in m}\max_{i\in m}|x_{0j}-x_{ij}|,$$

$$\Delta_{ij}=|x_{0j}-x_{ij}|,$$

ζ 为分辨系数，$0\leqslant\zeta\leqslant1$，取为0.5.

设有 m 个方案，计算各方案指标的灰色模糊隶属度，构成待选方案的判断矩阵 $\boldsymbol{U}=(\gamma_{ij})_{m\times4}$，$\gamma_{ij}$ 为方案的灰色模糊隶属度.

3.3.2 方案的灰色模糊优属度

优属度 L_i 是备选方案距理想最优方案的距离权[10]，

$$L_i=\frac{1}{1+[(1-I_i)/I_i]^2}. \tag{6}$$

式中：$I_i=\sum_{j=1}^{n}w_j\gamma_{ij}$，$w_j$ 是属性的权重，在木马检测中4指标权重使用两两比较法确定为

$$\boldsymbol{w}=[w_1\quad w_2\quad w_3\quad w_4]=[0.25\quad 0.25\quad 0.25\quad 0.25].$$

3.4 木马判定

定义危险指数为0.5，对于 $L_i\geqslant t$ 的行为序列判定为木马.

4 应用示例

1次木马检测中发现如下2个行为序列，如表3所示.

表3 木马行为检测结果

Tab.3 The detected result of Trojan actio

程序	行为序列1	行为序列2
网络通信	连接域名 u. qurl. f. 360. cn 接收数据大于发送数据	连接 vipdate. qpoe. com 发送数据大于接收数据
隐蔽运行	读写360Safe目录文件 读磁盘PE文件	读磁盘文档文件 截取用户屏幕
开机启动	注册表 CurrentVersion\Run 值启动 360tray. exe	注册表 CurrentVersion\Run 值启动 mskmonth. exe
自我防护	后台运行 360tray. exe	无图标窗口运行 iexplore. exe 动态链接库注入 iexplore. exe

木马判定步骤如下.

步骤1 计算行为序列评语. 对照表1，确定检出叶子方法的评语. 按照式(1)计算各个行为序列评语，得

$$\boldsymbol{A}_1=[\omega_3\quad \omega_3\quad \omega_3\quad \omega_4],\boldsymbol{A}_2=[\omega_3\quad \omega_4\quad \omega_3\quad \omega_5].$$

步骤2 对方案属性值进行规范化处理. 木马方案集 $A_u=\{A_1,A_2\}$，评价指标集 $V_u=\{V_B,V_C,V_D,V_E\}$，设计方案集 A 对评价指标集 V 的决策矩阵 $\boldsymbol{X}$ 为

$$\boldsymbol{X}=\begin{bmatrix}\omega_3 & \omega_3 & \omega_3 & \omega_4\\ \omega_3 & \omega_4 & \omega_3 & \omega_5\end{bmatrix}=$$

$$\begin{bmatrix}(0.5,0.5;0.2,0.2) & (0.5,0.5;0.2,0.2) & (0.5,0.5;0.2,0.2) & (0.8,1.0;0.2,0)\\ (0.5,0.5;0.2,0.2) & (0.8,1.0;0.2,0) & (0.5,0.5;0.2,0.2) & (1.0,1.0;0.2,0)\end{bmatrix}.$$

理想方案属性序列

$\boldsymbol{A}_0=[\omega_5 \quad \omega_5 \quad \omega_5 \quad \omega_5]=[(1.0,1.0;0.2,0) \quad (1.0,1.0;0.2,0) \quad (1.0,1.0;0.2,0) \quad (1.0,1.0;0.2,0)]$.

利用式(2)(3)(4)消除量纲并解模糊,得规范化解模糊决策矩阵 $\boldsymbol{X}^0$ 为

$$\boldsymbol{X}^0=\begin{bmatrix}0.515\,6 & 0.515\,6 & 0.515\,6 & 0.912\,5\\ 0.515\,6 & 0.912\,5 & 0.515\,6 & 1.000\,0\end{bmatrix}.$$

步骤 3　计算方案优属度进行木马判定. 将 $\boldsymbol{X}^0$ 中 2 个方案序列与理想参照序列

$$\boldsymbol{A}_0^0=[1 \quad 1 \quad 1 \quad 1]$$

比较,得

$$\boldsymbol{\Delta}=\begin{bmatrix}0.484\,4 & 0.484\,4 & 0.484\,4 & 0.087\,5\\ 0.484\,4 & 0.087\,5 & 0.484\,4 & 0\end{bmatrix},$$

则 $\Delta_{\min}=0$,$\Delta_{\max}=0.484\,4$,利用式(5)计算各属性值的灰色模糊隶属度,并构成判断矩阵

$$\boldsymbol{U}=\begin{bmatrix}0.333\,3 & 0.333\,3 & 0.333\,3 & 0.734\,6\\ 0.333\,3 & 0.734\,6 & 0.333\,3 & 1.000\,0\end{bmatrix}.$$

取属性权重向量

$$\boldsymbol{w}=[0.25 \quad 0.25 \quad 0.25 \quad 0.25],$$

利用式(7)计算可得 $I_1=0.433\,6$,$I_2=0.600\,3$. 利用式(5)计算得 $L_1=0.369\,5$,$L_2=0.540\,6$.

L_i 与危险指数比较可知行为序列 2 是木马发起的动作,基本顺序是 mskmonth. exe 开机启动,然后劫持 1 个 IE 浏览器主进程 iexplore. exe 要调用的 dll 文件,之后启动 iexplore. exe 连接域名 vipdate. qpoe. com 对应的主机接受控制.

5　结　论

针对计算机木马传统检测方法误报率和漏报率均无法完善解决的问题,提出了在木马攻击树分析基础上,使用主机资源访问行为、主机系统调度行为和网络行为检测技术实现对木马攻击树叶子节点方法的全部检测,从而构建可疑程序行为序列,然后通过计算被检行为序列与理想木马行为序列的灰色模糊的优属度,最后与危险指数比较进行木马判定. 通过示例验证了该方法的有效性.

参考文献:

[1] 李顺东,覃征,贾晓琳,等. 一种特洛伊木马的检测算法[J]. 小型微型计算机系统,2003,24(7):1371 - 1376.
Li Shundong, Tan Zheng, Jia Xiaolin, et al. A kind of algorithm for checking trojan horse[J]. Journal of Chinese Computer Systems, 2003,24(7):1371 - 1376. (in Chinese)

[2] 胡卫,张昌宏,马明田. 基于动态行为监测的木马检测系统设计[J]. 火力与指挥控制,2010,35(2):128 - 132.
Hu Wei, Zhang Changhong, Ma Mingtian. Design of a detection system of trojan horse based on monitoring dynamic behavior[J]. Fire Control & Command Control, 2010,35(2):128 - 132. (in Chinese)

[3] 李蓉,周维柏. 基于线程管理-端口截听的木马检测系统的设计[J]. 甘肃联合大学学报,2009,23(1):76 - 78.
Li Rong, Zhou Weibai. Design of trojan horse detecting system based on thread management and port intercepting[J]. Journal of Gansu Lianhe University, 2009,23(1):76 - 78. (in Chinese)

[4] 梁晓,李毅超,崔甲,等. 基于系统调用挂钩的隐蔽木马程序检测方法[J]. 计算机工程,2007,33(20):181 - 183.
Liang Xiao, Li Yichao, Cui Jia, et al. Stealthy trojan horse detection method based on system call hook[J]. Computer Engineering, 2007, 33(20): 181 - 183. (in Chinese)

[5] 杨玲,孟传良. 基于启发式分析的木马检测技术研究[J]. 现代机械,2006(4):61 - 63.
Yang Ling, Meng Chuanliang. Research on trojan horse detection based on heuristic analysis[J]. Modern Machine, 2006(4):61 - 63. (in Chinese)

[6] 闫峰,刘淑芬. 基于逃避行为检测的特洛伊木马技术研究[J]. 吉林大学学报:信息科学版,2007,25(6):641 - 645.
Yan Feng, Liu Shufen. Technique research of trojan horse based on escaping behavioral detection[J]. Journal of Jilin University: Information Science ed, 2007, 25(6):641 - 645. (in Chinese)

[7] Schneier B. Attack trees: modeling security threats[J]. Dr Dobb'S Journal, 1999(2):121 - 125.

[8] Liou T S, Wang M J. Ranking fuzzy numbers with integral value[J]. Fuzzy Sets and Syst, 1992, 50: 247 - 255.

[9] Bonissone P P. A pattern recognition approach to the problem of linguistic approximation in system analysis[C]// Proceedings of the 1979 International Conference on Cybernetics and Society. Piscataway: IEEE Service Center, 1979:793 - 798.

[10] 屈福政,费烨,王欣. 复杂机械方案多属性灰色模糊优选模型及应用[J]. 大连理工大学学报,2005,45(2):201 - 205.
Qu Fuzheng, Fei Ye, Wang Xin. Multi-attribute grey fuzzy optimal seleetion model complex mechanism design scheme and its application[J]. Journal of Dalian University of Technology, 2005,45(2):201 - 205. (in Chinese)

(责任编辑:刘芳)

基于行为序列灰色模糊判定的计算机木马检测方法

作者： 胡光俊， 宋伟航， 徐国爱， HU Guang-jun， SONG Wei-hang， XU Guo-ai

作者单位： 胡光俊,HU Guang-jun(北京邮电大学,网络与信息攻防技术教育部重点实验室,北京100876;公安部第一研究所,北京100048)， 宋伟航,SONG Wei-hang(公安部第一研究所,北京,100048)， 徐国爱,XU Guo-ai(北京邮电大学,网络与信息攻防技术教育部重点实验室,北京100876)

刊名： 北京理工大学学报 ISTIC EI PKU

英文刊名： TRANSACTIONS OF BEIJING INSTITUTE OF TECHNOLOGY

年，卷(期)： 2011,31(5)

参考文献(10条)

1. 李顺东;覃征;贾晓琳 一种特洛伊木马的检测算法[期刊论文]-小型微型计算机系统 2003(07)

2. 胡卫;张昌宏;马明田 基于动态行为监测的木马检测系统设计[期刊论文]-火力与指挥控制 2010(02)

3. 李蓉;周维柏 基于线程管理-端口截听的木马检测系统的设计[期刊论文]-甘肃联合大学学报 2009(01)

4. 梁晓;李毅超;崔甲 基于系统调用挂钩的隐蔽木马程序检测方法[期刊论文]-计算机工程 2007(20)

5. 杨玲;孟传良 基于启发式分析的木马检测技术研究[期刊论文]-现代机械 2006(04)

6. 闫峰;刘淑芬 基于逃避行为检测的特洛伊木马技术研究[期刊论文]-吉林大学学报(信息科学版) 2007(06)

7. Schneier B Attack trees:modeling security threats 1999(02)

8. Liou T S;Wang M J Ranking fuzzy numbers with integral value[外文期刊] 1992

9. Bonissone P P A pattern recognition approach to the problem of linguistic approximation in system analysis 1979

10. 屈福政;费烨;王欣 复杂机械方案多属性灰色模糊优选模型及应用[期刊论文]-大连理工大学学报 2005(02)

本文读者也读过(8条)

1. 王泽东.刘宇.朱随江.刘宝旭.潘林.WANG Zedong.LIU Yu.ZHU Suijiang.LIU Baoxu.PAN Lin 采用行为分析的单机木马防护系统设计与实现[期刊论文]-计算机工程与应用2011,47(11)

2. 颜会娟.秦杰.YAN Hui-juan.QIN Jie 基于非线性SVM模型的木马检测方法[期刊论文]-计算机工程2011,37(8)

3. 陈雷霆.张亮.CHEN Lei-ting.ZHANG Liang 人工免疫机制在木马检测系统中的应用研究[期刊论文]-电子科技大学学报2005,34(2)

4. 李焕洲.陈婧婧.钟明全.唐彰国.LI Huan-zhou.CHEN Jing-jing.ZHONG Ming-quan.TANG Zhang-guo 基于行为特征库的木马检测模型设计[期刊论文]-四川师范大学学报（自然科学版）2011,34(1)

5. 杨彦.黄皓.YANG Yan.HUANG Hao 基于攻击树的木马检测方法[期刊论文]-计算机工程与设计2008,29(11)

6. 陆军 浅谈木马的防御与查杀[期刊论文]-科技致富向导2011(9)

7. 张昊 木马技术发展的新趋势探讨[期刊论文]-科技创新导报2011(7)

8. 陈婧婧.李焕洲.唐彰国.钟明全 木马运行机制及行为特征分析[期刊论文]-计算机安全2009(10)