

基于交叉循环和改变数据关联的 移动代理迷乱保护方案

吴杰宏¹, 郭晓淳², 石祥滨³

(1 沈阳航空航天大学 工程训练中心, 辽宁 沈阳 110136;

2 沈阳广播电视大学 信息工程学院, 辽宁 沈阳 110003;

3 沈阳航空航天大学 计算机学院, 辽宁 沈阳 110136)

摘 要: 针对移动代理在异质网络环境中的安全问题, 提出了一种代码迷乱转换保护策略。代码迷乱技术应用于移动代理, 是对执行任务的移动代理的保护和隐藏模式的探索。该方案首先提出基于交叉循环迷乱和改变数据关联的移动代理保护策略, 接着阐述了交叉循环迷乱、多模块交叉循环迷乱以及改变数据之间内在关联的具体方法。实验证明, 该方案成功抵御了给定的 7 个 java 解码程序, 显示出比多层退出迷乱和单层退出迷乱方法的有效性。

关键词: 移动代理; 代码迷乱; 交叉循环迷乱; 扩展遗传树; 伪重构

中图分类号: TP393.08

文献标识码: A

文章编号: 1000-7180(2013)03-0008-04

MA Obfuscation Protection Scheme Based on Intersecting Loop and Varying Data Relationship

WU Jie-hong¹, GUO Xiao-chun², SHI Xiang-bin³

(1 Engineering Training Center, Shenyang Aerospace University, Shenyang 110136, China;

2 School of Information and Engineering, Shenyang Radio and TV University, Shenyang 110003, China;

3 Computer School, Shenyang Aerospace University, Shenyang 110136, China)

Abstract: Code obfuscation encryption protecting scheme is put forward, aiming to solve the security problems of Mobile agents (MA) migrating across heterogeneous network execution environments. Code obfuscation technology is applied to MA, and MA codes of executing task will be hided and protected. Firstly, mobile agent protection scheme based on intersecting loop obfuscation and varying data relationship is put forward in this paper. Secondly concrete methods of obfuscation protection scheme are introduced, and it is showed in experiment at last, 7 java decoders have been resisted using this scheme, which showed more validity than single-level exit obfuscation and multi-level exit obfuscation.

Key words: mobile agent; code obfuscation; intersecting loop obfuscation; extending inheritance tree; pseudo reconstruction

1 引言

移动代理(Mobile Agent: MA)是具有移动特性的智能 Agent, 它可以自主地在网络上从一台主

机移动到另一台主机, 并代表用户完成指定的任务, 如检索、过滤和收集信息, 甚至可以代表用户进行商业活动。由于移动代理必须在主机环境中运行, 完全受执行环境的控制, 很容易受到恶意主机的攻击, 因此移动代码的安全保护问题成为移动代理系统的安

收稿日期: 2012-06-25; 修回日期: 2012-07-19

基金项目: 国家自然科学基金项目(61170185); 辽宁省科技厅博士启动基金项目(20101082); 辽宁省教育厅科学技术项目(L2011030)

全研究中最棘手的问题^[1-3].

根据混乱转换的原则,本文提出一种新型的移动代理保护方案,通过改变数据关联和交叉循环混乱的方法来保护网络中执行任务的移动代理,增强了任务 MA 的安全性.

2 改变数据之间的内在关联

在面向对象的 Java 语言中,主要考虑的模块化和抽象的概念就是类.类是封装数据和方法的基本的抽象数据类型.我们编写了这样一个类 $C=(V, M)$, V 是 C 类的对象实例变量的集合, M 是它的方法集合.

对比传统概念的抽象数据类型, C_1 和 C_2 这两个类通过继承关系可以组成集合 (C_2 有一个类型为 C_1 的对象实例, C_2 通过添加新的方法和对象实例继承了 C_1). 借用参考文献[2]的记法,我们写了继承关系式 $C_2=C_1 \oplus \Delta C_2$, C_2 继承了它的父类 C_1 . $\oplus$ 符号表示合并父类和新属性 ΔC_2 的函数. $\oplus$ 的准确语义依赖于所使用的特定程序语言.在 Java 语言中,当应用于实例对象时, $\oplus$ 通常被解释成结合;当应用于方法时, $\oplus$ 被解释成叠加.

2.1 扩展遗传树方法

根据 Chidamber 矩阵, C_1 类的复杂程度随着它在继承树中的深度增加而增加,随着它直接子孙数目的增加而增加.如图 1(a)和(b)所示,有两种可以增加这种复杂度的基本方式:分裂一个类或者插入一个新的伪造的类.

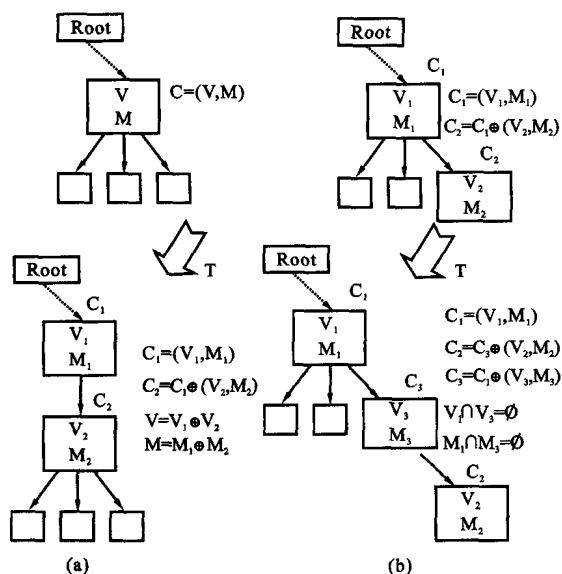


图1 扩展遗传树图示

如图 1(a),把 C 类分裂为 C_1 类和 C_2 类,并且不能把 C 类中的方法和实例对象移到它的结果类中,为

了解决这个问题,让 $C=(\{V\}, \{M\})$,方法 M 引用了实例对象变量 V ,注意 C 类的任何分裂都不能超出 V 的范围.例如,不能分裂 C 为 $C_1=(\{\}, \{M\})$, $\Delta C_2=(\{V\}, \{\})$, $C_2=C_1 \oplus \Delta C_2$ 等这样的组合形式.

为了解决上述分裂中遇到的问题,我们建立了一个类 C 的依赖关系图 G . G 中的节点是 C 中的成员和 C 本身.如果声明中有 a 到 b 的作用域的话,那么图 G 中就有一条边 $a \rightarrow b$.如果在图 G 中有一条路径 $C \sim > y$,那么 y 一定在子类 C_2 中声明了.如果在图 G 中有一条从 $x \sim > y$ 的路径,那么 x 和 y 一定在同一个类中声明,或者 x 在父类 C_1 中声明.如图 2 所示.

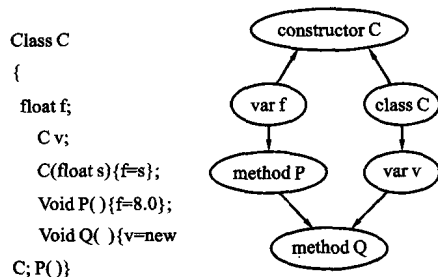
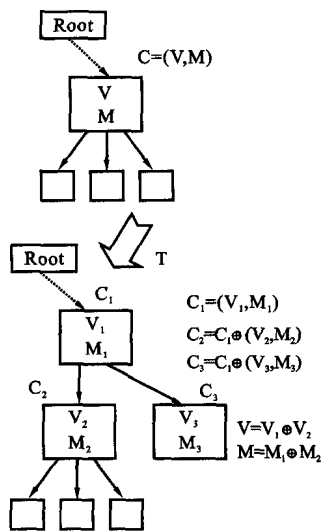


图2 类分解依赖图

类分裂的另外一个问题就是类的回弹能力,仅仅阻止解码程序来合并分裂的类是不现实的.为了防止解码,合并分裂和插入方法,如图 3 所示.还可以插入伪代码,看起来就像产生了所引入类的实例对象.例如,语句 $\text{if}(PF) x=\text{new } C_1$ 看起来就像产生了 C_1 类的一个实例.



的功能,第二阶段,这两个类的共同特征移入一个新的父类中. 伪重构就是这样一个相似的操作,它仅仅在没有共同行为的 C_1 和 C_2 类中执行. 如果两个类都有同一类型的实例对象,它们就可被移入新的父类 C_3 中. C_3 的方法可能是 C_1 和 C_2 中一些方法的组合.

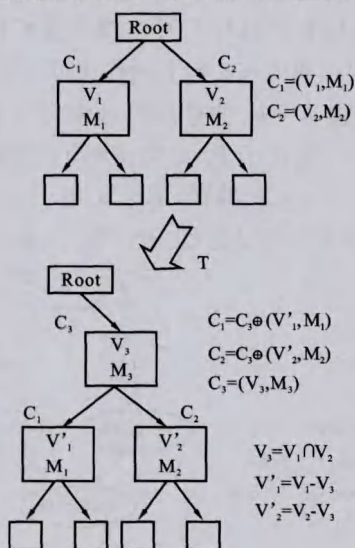


图4 伪重构图示

3 交叉循环迷乱

如果存在不合理的控制流,解码器重新构造 java 语句将会失败. 例如:原本不应该在 java 源代码里出现的控制流出现了,而一个专业的 java 编译器却绝不可能生成这样的结构. 交叉循环迷乱方法交叉了两个循环并把这种模式加进程序里. 为了跳过这种交叉循环,在程序中可引入一个假的模糊预测,这样就避免了程序在运行时进入到交叉循环模块中,可见,这种模糊预测对避开由 Java 验证程序引起的验证失败来说很重要.

虽然这么做可以使解码失败,但是迷乱代码被以这样一种形式放在一起以至于它们可以很容易的被检测到和移走. 一种解决方案就是制造一些能实际应用的便宜的、有弹性的、隐密的结构,以此来防止模式匹配袭击,可以参考 Collberg^[4] 等的提议. 本文使用另外一种迷乱方案——多模块交叉循环迷乱. 如图5所示,首先分裂原始程序流和交叉循环,接着在复杂的程序流中插入一些 goto 语句和模糊预测指令,然后把它们合并在一起形成了一个更加复杂的结构,这时解码程序的模式匹配侦测便不能起作用了.

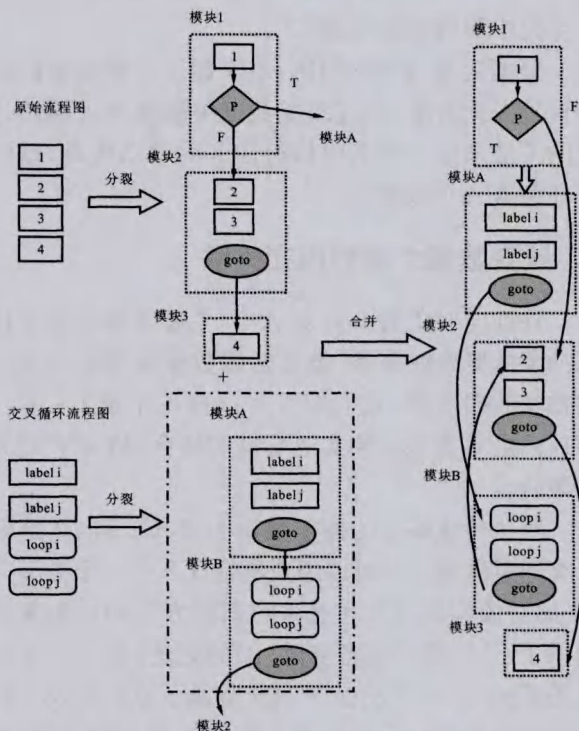


图5 多模块交叉循环迷乱转换过程

4 实验测试

测试结果表明,如果不应用迷乱方法,6个解码器能够重新构造初始源代码^[3-5]. Dava 解码了多层退出迷乱和单层退出迷乱方法^[6]. 改变数据之间的关联和交叉循环迷乱成功地抵御了所有的解码程序,显示出比多层退出迷乱和单层退出迷乱方法的更高有效性.

5 结束语

本文提出了改变数据之间内在关联和迷乱控制结构的主动保护策略,通过对派发前的 MA 进行数据和控制迷乱,可以有效抵制网络中恶意主机的攻击. 本方案和文献^[7]提出的时间核查方案合并将发挥更强的保护作用,不仅可以抵御攻击,还可以快速确定有恶意行为的主机.

由于数据迷乱和控制迷乱组合在一起改变了数据类型和程序体,为了使程序更加复杂,两种迷乱技术在字节码中引入了额外的计算,这些额外计算将增加字节码的大小;此外,额外的计算将使程序运行时的效率降低. 因此,今后的研究将从空间和时间上来提高代码迷乱转换的质量.

参考文献:

- [1] 张云勇,刘锦德. 移动 agent 技术[M]. 北京:清华大学

出版社,2003.

- [2] Lan P. Of graphs and coffi grounds; decompiling Java [R]. McGill UNiversity School of Computer Science, Sable Research Group, 1998.
- [3] Sureshot Software Co., Ltd. Cavaj - the java decompiler[EB/OL]. (2002-07-11)[2012-06-25]. <http://www.bysoft.se/sureshot/cavaj/>, v1.
- [4] Cowley M. Front End plus - the java decompile[EB/OL]. [2012-05-17]. http://www.softpile.com/Development/Java/Review_03171_index.html, v1.00, 2001.
- [5] Lemaire B. NMI's java class viewer - the java decompiler[EB/OL]. [2012-06-20]. <http://www.jreveal.org/cgi-bin/resource.pl?resid=4397>, v4.7.

- [6] Peterson W W, Kasami T, Tokura N. On the capabilities of while, repeat, and exit instructions[J]. Commun. ACM, 1973, 16 (8): 503 - 512.
- [7] Wu Jiehong, Chang Guiran, Li Jia. A scheme for protecting mobile agents based on combining obfuscated data and time checking technology[C]// Proceedings of the 3rd International Conference on Intelligent Information Hiding and Multimedia Signal Processing. Kaohsiung, Taiwan, 2007(1):221-224.

作者简介:

吴杰宏 女,(1971-),博士,副教授.研究方向为移动代理的安全、动态频谱存取协议及算法.

(上接第7页)

- [7] 盛苏英,吴新华.一种混沌图像加密算法的研究与改进[J].微电子学与计算机,2010,27(10):61-64.

作者简介:

林 纯 女,(1980-),硕士,讲师.研究方向为混沌控制.

王建平 女,(1981-),硕士,讲师.研究方向为图像处理.

马卫国 女,(1976-),博士,讲师.研究方向为混沌同步、保密通信.

陆国平 男,(1965-),博士,教授.研究方向为非线性控制、智能控制.