对象监控的协同入侵检测*

滕少华，伍乃骐，张 巍，傅秀芬
（广东工业大学 计算机学院，广东 广州 510006）

摘 要： 分析现有入侵检测技术存在的问题，主要在于数据的获取及检测方法上。据此，提出了一种解决这些问题的新途径，就是紧紧抓住入侵检测的本质问题，从对象分类入手，给出了一个协同入侵检测模型，描述了该模型的各个部件。设计了入侵事件检测代理及融合中心，重点阐述了如何应用场景与自动机技术，将检测一个入侵的方法扩展到检测一类入侵的问题，对可序列化的攻击，文章提出的检测方法能检测其变种攻击。实验检验了方法的有效性。

关键词： 对象；入侵检测；状态转换；场景；融合
中图分类号： TP393 **文献标识码：** A **文章编号：** 0529-6579（2008）06-0076-06

入侵检测（intrusion detection）[1]是识别那些未经过授权而使用计算机系统的个体和那些经过授权但是滥用权力的个体的技术。入侵检测技术分为[1-3]：滥用入侵检测（misuse - based intrusion detection）和异常入侵检测（anomaly - based intrusion detection）。

在众多的入侵检测系统中，基于特征与规则的入侵检测是入侵检测领域内最为有效及使用最广泛的技术之一，被广泛用于滥用入侵检测系统中，仍是保障计算机系统及网络安全的最主要措施之一。但它们仍存在如下缺陷[1]：第一，只能检测已知攻击，对新出现漏洞的攻击或旧漏洞的新攻击或变种攻击失效。原因是规则或模式库中缺乏攻击的特征模式；第二，系统的有效性依赖于训练数据质量，规则与提炼的审计记录之间往往是一一映射关系，这导致入侵序列中的一个微小变化将使基于规则的入侵检测系统失效；第三，没有能力预测将要发生的危险，只能在危险发生后，进行报告及结束入侵活动；第四，规则库既不容易创建也不易更新，规则更新需要有经验的规则库程序员。而入侵检测系统的规则需要经常更新，这给系统使用造成障碍。

为此，许多学者从不同角度研究入侵检测，提出了许多方法和技术[1,4-5]，有关这方面的讨论参见文［1］。本文提出了一种方法 - 基于对象监控技术的协同入侵检测 CIDMOM（Cooperative Intrusion Detection Model Based On Object Monitoring）。因为入侵检测技术的目的是识别并阻挡非法用户对象对系统的使用，识别并跟踪合法用户对象的越权行为。由此本文对不同种对象分别采用不同处理办法，通过检测动态栈是否溢出、通信端口活动情况及用户对象越权行为等来检测入侵活动。

本文与前人的工作有所不同。第一，从分类出发，提出了适用于入侵检测的对象分类技术；第二，数据来源更广泛，除网络数据包与审计记录外，还有主机状态信息；第三，检测方法不同，本文通过跟踪对象的调用行为及调用序列，及时发现入侵活动；这不同于通过模式匹配或统计分析技术的入侵检测；第四，解决变种攻击检测问题，将检测一个入侵问题扩展到检测一类入侵问题，从根本上解决入侵方法的变种及变形检测问题；文献［6］给出了 class 及入侵序列的概念，但未将命令序列扩充到各种攻击工具及其等价变种；第五，新增预警机制，在检测入侵的场景中，通过增加临界状态，引入预警机制，及时终结攻击活动。这在以往的技术中未见介绍；第六，不受时空约束，采用自动机与数据融合技术检测入侵，不受时间及入侵序列长度的限制，具有更大实用性。本文提出的方法已通过实验验证其有效性。

1 分布式协同入侵检测

当前的网络环境要求入侵检测系统从不同子网

* **收稿日期：** 2008 - 09 - 10
基金项目： 国家自然科学基金资助项目（60474061）；广东省自然科学基金资助项目（06021484）；广州市越秀区科技计划资助项目（2007 - GX - 023）
作者简介： 滕少华（1962年生），男，博士，教授；E-mail：shteng@gdut.edu.cn

及主机所发生的入侵迹象中，判断入侵情况，及时预警、检测入侵，并做出相应的响应。然而随着网络结构更加复杂，对入侵检测技术提出了更高的要求。单个入侵检测器难以保障网络安全，多代理协同入侵检测被需要。

1.1　协同入侵检测体系

基于对象监控技术的分布式协同入侵检测模型由传感器、事件生成器（群）、负载均衡器、通信模块、事件检测代理（群）、融合中心（群）、监控中心、响应单元等部分组成，其总体架构采用 4 层分布式结构，如图 1 所示，分别是传感器、事件生成器（群）、事件检测代理（群）和融合中心（群）。

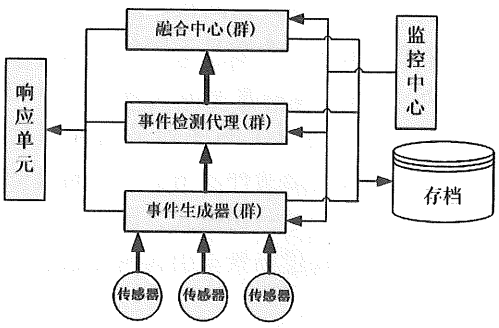

图 1　分布式协同入侵检测体系结构

Fig. 1　Distributed cooperative intrusion detection architecture

1.2　各组件简介

传感器用于收集数据，主要收集网络数据包、日志和其他信息，提交给事件生成器。

事件生成器（群）接收传感器提交的数据，依据数据来源，分类提取、检测、过滤并组织数据，过滤掉正常用户数据，剔除黑客网址发来的信息及检测到的入侵数据。对不确定数据，生成可疑入侵事件，根据可能的攻击对象做出初步判断，转发到相应的事件检测代理。

事件检测代理（群）接收事件生成器（群）传来的可疑入侵事件，按照一定的方法对可疑入侵事件进行分析与处理。其检测结果分为三种：①当检测到正常用户行为时，将结果同相应事件存档；②当检测到攻击时，保存入侵事件及检测结果，转响应单元处理；③对不能决策的可疑入侵数据，交融合中心做进一步分析。

融合中心对事件检测代理上传的可疑入侵数据进行预处理，剔除错误及冗余数据，然后进行相关性分析（时空融合及内容融合），进一步简化数据，最后按照融合算法的结果做检测决策，融合中心有三种检测结果：①和②类似于事件检测代理；③对一些融合中心仍不能判断的可疑入侵数据，通过人机交互做出相应的处理。比如：建议安全管理人员密切监视相应事件，观察事件发展动态；或者通过其他途径，调查核实事件的对象情况。

响应单元根据事件检测代理或融合中心的分析结果，依据入侵事件的严重程度，选择相应的处理应对。本模型可以做出如下响应：记录异常信息、发送日志文件到指定邮箱、通知安全管理人员、断开某个 TCP 连接、终止非法进程运行或删除某个应用程序、中断服务等。

监控中心负责监控、管理、协调各事件检测代理（群）的工作。

负载均衡器负责各事件检测代理的任务分派，监控各事件检测代理的运行情况，接受事件检测代理的通信请求与服务。

通信模块负责事件检测代理之间、事件检测代理与融合中心之间的通信。系统交换信息有两种：可疑入侵事件信息报文和会话控制信息报文[1]。前者用于传送可疑入侵事件信息，后者用于传送控制信息和时钟同步等信息。本文借用 UDP 协议通信。

2　攻击分类

2.1　常见攻击分类简介

中外学者从各种角度对攻击方法的分类问题展开了研究，本文分析了若干种有代表性的分类法，这些分类法在入侵检测领域内发挥着重要作用，有的工作是开创性的，有的分类体系与分类思想正被应用于许多入侵检测系统中，比如 Anderson[7] 的工作是开创性的，后来 Neumann 和 Knight 等[8-9] 进行来了细化与扩展，SRI 和 Purdue 大学的分类观点被用于 MIDAS、IDES 和 AAFID 等入侵检测系统中，缺点假设分类方法被用于系统安全评测中。

Anderson 与 Neumann 等从计算机滥用角度出发，对入侵行为进行了分类，这种分类体系正应用于当前的许多入侵检测系统中，诸如 MIDAS、Snort 和 IDES 等。但该分类体系仍存在局限[1]。①分类中引入了硬件方面的损坏；②分类不完备[1, 10]；③分类存在重叠，互斥性[1, 9] 有问题。Howard 从攻击过程分类[1]，存在如下局限：①分类中的攻击者、攻击工具和攻击目的等信息难以获取；②分类不互斥[1]。Kumar、Bishop[1, 11] 和 Richardson 等[1] 从攻击特征分类，他们的工作适合于构建基于特征的入侵检测代理，但仍存在分类互斥与重叠问题，并且当日志文件缺失时，无法检测入侵

问题。Linde 等[1]采用缺陷假设模型及缺陷假设方法学进行分类，其分类适用于安全性评估，通过扫描可列出计算机系统的缺陷及漏洞，建立计算机防护体系。王晓程等[12]给出了 ESTQ（Event，State，Time，Quantity）网络攻击分类法，利用统计来检测网络攻击，有利于检测扫描、拒绝服务及重复性攻击，但容易被误解为发生多个攻击，存在重复报警和难以实时问题。

上文对典型的几种攻击分类进行了分析，可知：①各人的分类都存在差异，并有其侧重。每种分类与检测的入侵及攻击方法有关（至少支持他们想处理的问题）。②尚不存在一种通用的分类，支持所有入侵检测。另外当前的攻击往往是病毒与黑客程序联合，网络与主机攻击并行，分布式协同攻击与其它攻击混杂，因此以前的分类研究不仅存在完备性及互斥问题，还存在数据融合问题，即将分布式协同攻击（包括网络与主机攻击）的检测结果进行融合。

2.2 O-R-M-C 分类体系

本文提出了一种“对象－结果－机理－特征”的 O-R-M-C（Object－Result－Mechanism－Character）分类方法[1]。此处，①对象（Object），指系统中启动的进程、登录系统的用户、系统中文件、程序、数据、计算机、网络等；②结果（Result），指攻击产生的后果，如缓冲区溢出、非法获取了 root 用户权限等；③机理（Mechanism），指攻击的构造、攻击原理、方法、过程及手段等；④特征（Characteristics），指经分析、提取获得的攻击特征或攻击序列，该序列有助于将检测某个入侵扩展到检测某类入侵，亦有助于将异常检测转为滥用检测。

对象分为主机与网络两大类，帐户、文件、进程、系统资源、网络与网络服务五小类；攻击结果从攻击造成的影响（信息泄漏或篡改、非法利用服务、拒绝服务、非法提升权限）、攻击的传播性、攻击的破坏强度三方面分析；攻击机理分为网络与主机攻击。

3 入侵事件检测代理

随着网络的发展及应用深入，网络攻击呈现复杂性及多样性。为了检测入侵，对攻击事件分类很有必要。依据 O-R-M-C 分类，入侵事件检测代理被分为特征、规范、统计及基于场景检测四类。

3.1 事件检测代理

特征检测代理基于模式或规则匹配，如匹配成功，则报告入侵事件。规范检测用于应对木马及病毒攻击，需要预先保存系统的配置信息，通过比较进行检测。统计检测：在一给定时间间隔内，当收到的数据包数超过某给定阈值时，认为发生攻击事件。如果是由内向外发送信息，则发生木马攻击；否则可能是扫描或拒绝服务攻击。基于场景的检测被用于应对可序列化的攻击，包括协同攻击、多个会话完成的一次攻击、变种攻击等，本文利用对象监控技术，跟踪对象行为及其状态变迁来检测入侵。

3.2 基于场景的入侵检测

3.2.1 入侵场景与衍生攻击

由于许多攻击方法都存在变种攻击，表1列出了 BSD Unix 系统的一个漏洞[1,6]，执行序列 S_1 S_2 S_3 S_4 S_5 后，将获取 root 用户访问权。如执行 S_3 S_1 S_2 S_4 S_5或 S_1 S_3 S_2 S_4 S_5或 S_1 S_3S_3 S_3 S_3 $S_2S_2S_2$ S_2 S_4 S_5，同样可获取 root 用户访问权。但是上述4个序列的顺序及序列中元素个数是不同的。实际上，从 S_1 S_2 S_3 S_4 S_5 出发，可以派生出无数个具有相同执行效果的序列，所有派生的序列是前面序列的变种，由此产生的攻击是变种攻击。基于特征的检测方法，由于不可能穷尽一切模式，因而无法应对变种攻击。本文通过构建场景与引入自动机，解决了此类攻击的检测问题。

表1 获取 root 用户 shell 文件访问权的命令序列[1]

Tab. 1 An intrusion scenario that one can get unauthorized access of shell file for root user

Step	Command	操作说明
S_1	cp/bin/csh/usr/spool/mail/root	假定没有邮件
S_2	chmod 4755 /usr/spool/mail/root	设置 root 文件的属性
S_3	touch x	创建一个空文件 x
S_4	mail root < x	发送空文件 x 到 root
S_5	/usr/spool/mail/root	运行 root 文件

3.2.2 状态转换法检测入侵

状态转换分析使用状态转换图（state transition diagrams）来描述对象行为[1,13]，入侵过程由一系列导致系统从初始状态转换到终止状态的对象行为组成。初始状态表示入侵发生之前系统所处的状态（即安全状态 S-safe state），终止状态表示危及安全状态（即 V-vulnerable state）[1]。系统状态用对象属性来描述，对象行为或施加给对象的操作导致系统状态改变。对一个入侵场景，在初始与终止状态之间有一组中间状态，用以标识关键路径。

例如，表1攻击序列可用如图2所示的状态转换图来识别。其中 S 为初始状态，C 为临界状态（终止状态前的一个状态），V 为终态，S_1、S_2和

S_3为中间状态，弧上标记 S_1、S_2、S_3、S_4、S_5分别表示表 1 中相应的操作。

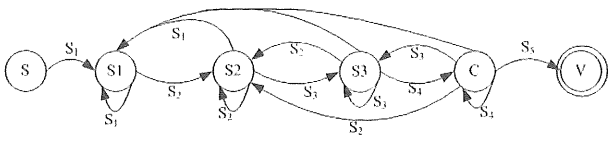

图 2　识别序列 $S_1S_2S_3S_4S_5$的状态转换图

Fig. 2　State transition diagram of identifying sequence $S_1S_2S_3S_4S_5$

3.2.3　场景及其组成

场景就是在已知一个问题解的基础上，通过对解序列同构变换及拓扑排序，扩充到包含求解一类问题的方法。此处表示解决已知攻击及其所有变种攻击的检测问题。

场景生成需要数据库、学习机、自适应器 3 个模块[1]，三者之间的关系如图 3 所示。

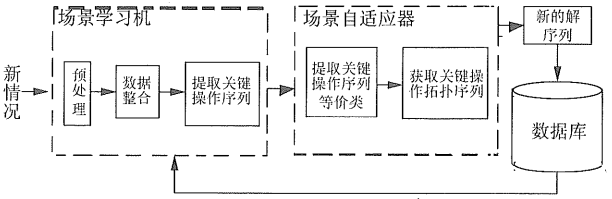

图 3　场景生成模块

Fig. 3　Scenario generation module

场景学习机由预处理、数据整合和提取关键路径三部分组成。

对于表 1 的入侵场景，假设收集到序列 $S_1S_1S_1S_2S_2S_2S_3S_3S_3S_4S_5$，经提取后，得到关键操作序列为 $S_1S_2S_3S_4S_5$。

表 1 的入侵场景关键路径是 S_1 S_2 S_3 S_4 S_5，其中 S_1、S_2和 S_3 之间存在偏序关系，S_1与 S_2 是全序关系，由此可得出表 1 入侵场景的所有拓扑序列为：① S_1 S_2 S_3 S_4 $S_5$② S_1 S_3 S_2 S_4 $S_5$③ S_3 S_1 S_2 S_4 S_5。

3.2.4　构建基于场景的检测自动机

对于任意一个可序列化的攻击，我们可以获得关键路径，进而得到所有可能的关键操作拓扑序列。因而能创建一个识别该入侵场景的所有关键路径的有穷自动机。

创建识别入侵场景的有穷自动机步骤如下：

第 1 步：从入侵场景库取一元组；

第 2 步：取出该入侵场景的所有拓扑序列；

第 3 步：按拓扑序列第 1 个元素分组，将所有第 1 个元素相同的拓扑序列归入同一组；

第 4 步：对每个分组 i，考察拓扑序列的第 2 个元素，将所有第 2 个元素相同的拓扑序列归入同一小组 $i-k$；…，以此类推，直至所有拓扑序列归入相应的分组。

第 5 步：创建一个开始结点，即根结点 S_0；

第 6 步：以 S_0 为根，构造第 1 层子树，其弧上标记是各分组的命令或操作，即拓扑序列的第 1 个命令或操作；

第 7 步：以各子树为根，构造第 2 层子树，弧上标记是拓扑序列的第 2 个元素；

第 8 步：以此类推，直至所有分组都处理完；

第 9 步：考虑自动机的冗余识别问题，做出能识别重复操作的自动机；

第 10 步：依据拓扑序列，构造相应的状态转换分析器。

检测表 1 入侵场景的有穷自动机如图 4 所示。图中，S、C1、C2、V、Q1、Q2、Q3、Q4、Q5、Q6、Q7 和 Q8 是状态；S 是开始状态，C1 和 C2 是临界状态，V 是终止状态；弧上标记 S_1、S_2、S_3、S_4 和 S_5 为表 1 操作或命令，Others 表示执行了退出或系统恢复操作。

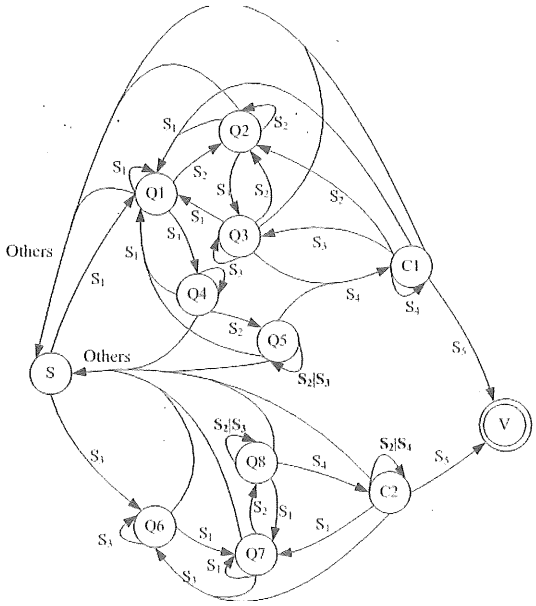

图 4　检测表 1 的入侵场景的有穷自动机

Fig. 4　Detection automata for intrusion scenario in table 1

4　对象监控技术

从一个入侵场景出发能够确定关键路径，并利用状态转换来表示，如果加入一组断言，采用类似于语法制导技术进行检测。即当通过一个关键操作到达新状态时，都执行相应的语义子程序，检查对象是否变化，实现对象监控技术。带语义子程序的

检测自动机如图5所示。对于表1的入侵场景，带语义子程序的状态自动机可类似得到，参见文献[1]。

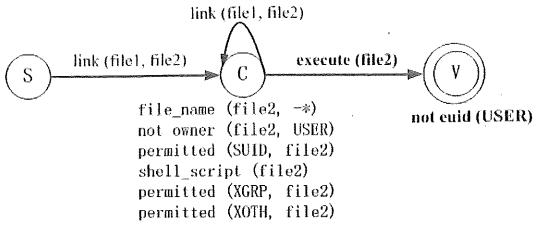

图5 基于对象监控技术的入侵场景检测自动机

Fig. 5 Detection automata for intrusion scenario based on object monitoring

5 融合中心

融合中心由预处理、相关性分析、带权融合模块组成。各部件及其联系参见图6。

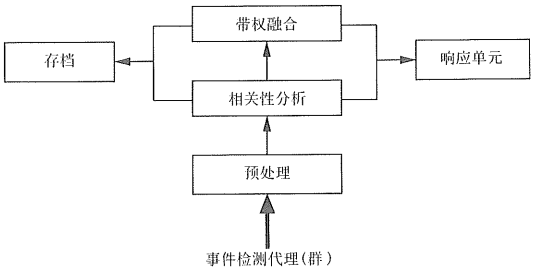

图6 融合中心各部件及其联系

Fig. 6 Fusion center and components

预处理器接收各入侵事件检测代理传来的信息，按照数据的空间信息分组（目的主机地址、目的网络地址、源主机地址、源网络地址、目的端口、源端口），再对数据按时间顺序排序，生成可疑事件集合。

相关性分析：从可疑事件时间、空间及内容上进行相关性分析，剔除冗余报警事件，以获得更准确的结果。比如慢扫描攻击[1]采用轮流扫描网络内多个主机，使得对每个主机发起连接请求的延时较大，不易被基于统计的入侵检测器检测。但当进行时空融合后，这种扫描攻击就难遁其踪。又如一个场景检测到扫描攻击，另一个场景检测到IIS攻击，如果数据包源地址相同，且扫描攻击在前，IIS攻击在后，则这两者很可能属于同一次攻击行为。

6 攻击与检测实验

实验室中6台计算机分别安排如下：①1台机器安装服务器Windows NT 5.0操作系统，并安装防火墙及自行开发的入侵检测模型CIDMOM（Cooperative Intrusion Detection Model Based On Object Monitoring）；②2台机器安装攻击软件；③3台机器安装检测代理。所有计算机通过TCP/IP网络连接。

实验1：拒绝服务攻击软件DDoS v1.4[14]，该软件集成了4种攻击，程序分为Client端和Server端，Server端安装在跳板机器上，执行后将自动安装为NT服务程序，并删除自身。实验中，一台机器运行Server端，另外两台运行Client端。注意Server端机器不能运行防火墙、木马查杀工具或入侵检测系统等。检测结果如图7所示：

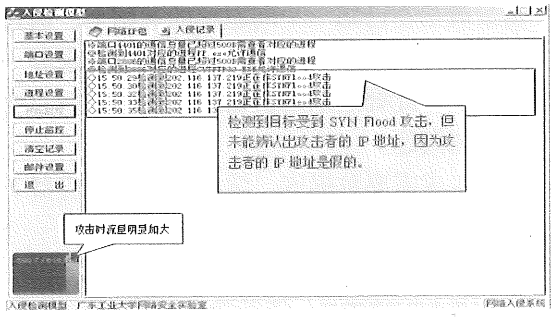

图7 拒绝服务攻击检测图

Fig. 7 Detecting Denial of Service

实验2：植入HorseTest木马[1]，HorseTest没有把信息写入到注册表或Win. ini、System. ini等文件中，因而防病毒软件和木马查杀工具都不能检测。CIDMOM通过监控对外的进程通信，发现HorseTestSrv进程正在非法对外进行通信，因而根据设置停止该进程工作。实验结果如图8所示，检测到如下信息：

※端口15334的通信总量已超过500B需查看对应的进程

▲检测到15334对应的进程HorseTestSrv. exe不允许通信，正停止其运行！

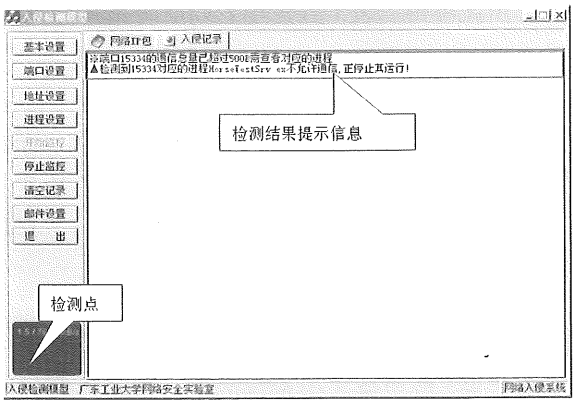

图8 检测HoseTest木马攻击

Fig. 8 Detecting HoseTest

7 结束语

依据 O-R-M-C 分类，我们正在建立并逐步完善协同入侵检测模型，通过将 Unix 系统的常见命令划分同构类，对一些关键操作进行监控，已获得了好的检测效果，下一步将继续展开并深化对象监控技术在入侵检测领域中的研究，期望进一步改善入侵检测模型的效果。

参考文献：

[1] 滕少华. 基于对象监控的分布式协同入侵检测 [D]. 广州：广东工业大学，2008.

[2] 马恒太，蒋建春，陈伟锋，等. 基于 Agent 的分布式入侵检测系统模型[J]. 软件学报，2000，11(10)：1312 - 1319.
MA H, JIANG J, CHEN W, et al. Distributed model of intrusion detection system based on agent[J]. Journal of Software, 2000,11(10):1312 - 1319.

[3] PENG N. Abstraction - based intrusion detection in distributed environments [D]. George Mason University, 2001.

[4] 苏璞睿，李德全，冯登国. 基于基因规划的主机异常入侵检测模型[J]. 软件学报，2003，14(6)：1120 - 1126.
SU P, LI D, FENG D. A host-based anomaly intrusion detection model based on genetic programming[J]. Journal of Software, 2003,14(6):1120 - 1126.

[5] 蔡忠闽，管晓宏，邵萍，等. 基于粗糙集理论的入侵检测新方法[J]. 计算机学报，2003，26(3)：361 - 366.
CAI Z, GUAN X, SHAO P. et al. A new approach to intrusion detection based on rough set theory[J]. Chinese Journal of Computers, 2003, 26(3):361 - 366.

[6] ESMAILI M, SAFAVI - NAINI R, BALACHANDRAN B, et al. Case - based reasoning for intrusion detection [C]. 12th Annual Computer Security Applications Conference, San Diego California, 1996:214 - 223.

[7] ANDERSON J P. Computer security threat monitoring and surveillance [R]. Fort Washington. PA, April, 1980.

[8] NEUMANN P G, PARKER D B. A summary of computer misuse techniques [C]. In 12th National Computer Security Conference, 1989:396 - 407.

[9] KNIGHT E. Computer vulnerabilities[M]. http://www.ussrback. com/docs/papers/general/ compvuln _ draft.pdf, 2008 - 04 - 06.

[10] LOUGH D L. A taxonomy of computer attacks with applications to wireless networks [D]. Virginia Polytechnic Institute and State University, 2001.

[11] KUMAR S. Classification and detection of computer intrusion [D]. Purdue University, 1995.

[12] 王晓程，刘恩德，谢小权. 攻击分类研究与分布式网络入侵检测系统[J]. 计算机研究与发展，2001，38(6)：727 - 734.
WANG X, LIU E, XIE X. Attack classification research and a distributed network intrusion detection system[J]. Journal of Computer Research and Development, 2001, 38(6):727 - 734.

[13] ECHMANN S T. The STATL attack detection language [D]. University of California Santa Barbara, 2002.

[14] http://www. cnd8. com/sort/247_2. htm, 2008 - 04 - 06.

Cooperative Intrusion Detection Based on Object Monitoring

TENG Shao-hua, WU Nai-qi, ZHANG Wei, FU Xiu-fen

(School of Computer, Guangdong University of Technology, Guangzhou 510006, China)

Abstract: In order to solve some present problems for intrusion detection, this text makes an attempt. With the help of O-R-M-C (Object, Result, Mechanism, Characteristic) classification, we give a model of cooperative intrusion detection and show its components and architecture. Detection agents for intrusion events and fusion center have been designed in the paper. Specially, basing on scenario and automata, we implement to detect a known attack and attacks of its varieties. At last, the detect method is verified by experiments.

Key words: object, intrusion detection; state transition; scenario; fusion