主动知识库系统在 IDS 中的应用研究

高秀峰　胡昌振
（北京理工大学信息安全与对抗技术研究中心　　北京　100081）

〔摘要〕 研究了主动知识库并将其应用于 IDS 中，利用其主动功能提高 IDS 的检测效率；将 ECA 规则引入到 IDS 中，并对系统动态特性和静态特性进行了分析，以提高入侵检测的能力。
〔关键词〕 IDS　主动知识库系统　ECA 规则　　〔中图分类号〕 TP393.08
〔文献标识码〕 A　　〔文章编号〕 1000-7857(2005)03-0028-04

A STUDY ON ACTIVE KNOWLEDGE BASE SYSTEM APPLIED IN IDS

GAO Xiu-feng　HU Chang-zhen
(Information Security & Antagonism Research Center, Beijing Institute of Technology, Beijing 100081, China)

Abstract: Based on the study to the Active Knowledge Base System (AKBS), the paper applies AKBS in the IDS. With some active functions of AKBS, it can improve the detection efficiency of IDS. When the ECA rules are applied to IDS, and the dynamics characteristic and static characteristics of the system are analyzed, the capability of IDS can be greatly improved.
Key Words: Intrusion Detection System(IDS), Active Knowledge Base System(AKBS), ECA Rule
CLC Number: TP393.08　　**Document Code:** A　　**Article ID:** 1000-7857(2005)03-0028-04

1 前言

在网络安全领域，作为一种积极主动的安全防护技术，入侵检测提供了对内部攻击、外部攻击和误操作的实时保护，可在网络系统受到危害之前拦截和响应入侵。因此，入侵检测系统(Intrusion Detection System，简称 IDS)体系结构及其检测技术，成为当前网络安全研究的热点。异常检测和滥用检测是 IDS 常用的两种检测技术，但由于这两种检测技术都存在固有的不足，当前基于这两种技术的各种检测方法在实际应用中都不能达到令人满意的效果。

近年来，入侵技术无论从规模与方法上都发生了较大的变化，主要向着综合化与复杂化、规模扩大化、分布化以及入侵主体对象的间接化发展，因此，IDS 也相应地朝着分布式、智能化及技术综合化方向发展。由于知识库在入侵检测系统中有着举足轻重的作用，随着 IDS 的发展，传统知识库显现出明显的不足。这是因为传统知识库本身是被动的，它只能根据用户的命令被动地提供服务；用户给什么命令，系统就做什么动作，丝毫不会根据知识库的外部环境或内部状态变化等灵活、主动地工作。比如，它做不到主动提出警告，主动实现某些动态修改和使用等功能[1]。

本文将主动知识库系统应用到 IDS 中，利用其主动功能不但可以提高 IDS 检测效率，还可以使其智能化。同时，利用 ECA 规则(Event-Condition-Action Rule)机制表示检测知识，可以进一步提高 IDS 检测能力。

2 主动知识库系统简介

2.1 主动知识库系统结构

一个主动知识库系统(AKBS)由一个传统知识库系统(KBS)和一个事件驱动的知识库(EB)(简称事件库)及相应的事件监视器(EM)组成，可用公式表示为[2]：

AKBS=KBS+EB+EM

其系统结构如图 1 所示。

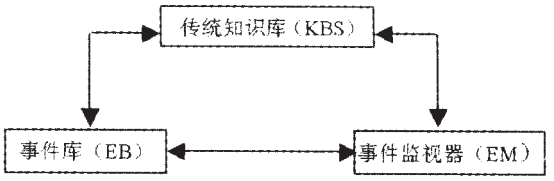

图 1　主动知识库系统结构

其中，EM 是一个随时监视 EB 中的事件是否已经发生的监视模块，一旦监视到某事件发生，就会主动触发系统，并按照 EB 中指明的相应知识执行其中预先设定的动作。事件库由系统和用户定义的各种事件驱动的规则组成，主动规则一般采用 ECA 规则，其表示形式为：

RULE <规则名>[(<参数>,…)]

收稿日期：2005-01-31
基金项目：国防科技基础研究项目
作者简介：高秀峰，男，1973~；北京市中关村南大街 5 号北京理工大学机电学院，博士研究生，研究方向为网络安全技术；E-mail: gxf_tsg@sohu.com
胡昌振，男，1967~；北京理工大学机电学院，教授，研究方向为网络安全技术与应用；E-mail: chzhoo@public.bta.net.cn

WHEN <事件>
IF <条件 1> THEN <动作 1>;
……
IF <条件 n> THEN <动作 N>;(n≥1)
END-RULE [<规则名>]。

2.2 主动规则的触发事件[3]

定义 1 触发事件:能引起主动规则触发的相关事件称为触发事件。

主动规则的事件可以分为两种:原子事件和复合事件。事件具有"原子性"——在某一时刻,或者完全发生,或者根本不发生,没有第三种状态。

定义 2 原子事件:原子事件(Primitive Event)是规则系统预先定义的,可以按照其性质分成基于不同的类型。在关系数据库中,原子事件可以分为:数据操纵类;事务类;时序类。

定义 3 复合事件:系统规定的事件操作符把若干成分事件(原子的或复合的)联结起来,作为单个事件处理,称为复合事件。复合事件的发生也具有"原子性",同样可以用事件修饰符界定具体发生时刻。复合事件的组成用事件表达式表示,事件表达式的语义表达能力取决于系统支持的事件操作符。

定义 4 主动规则的触发:当触发事件产生时,若触发事件与某个主动规则的事件定义相匹配,则称该主动规则被触发,整个触发事件与规则的事件定义匹配过程称为主动规则的触发。

2.3 主动知识库实现途径

主动知识库系统一般可以有以下 3 种实现途径。

(1)改造的途径:原有知识库管理系统+事件监视器(具有较高运行优先级)。

(2)嵌入主动程序设计语言的途径。把一般程序设计语言改造成一种主动程序设计语言,或设计实现一种主动程序设计语言,然后按传统方法(设计一个接口)把知识库操作嵌入其中执行。该途径已由主动程序设计语言将事件库分成块,分布在各个过程或对象(当采用面向对象范式时)中,运行效率可望大大提高。

(3)重新设计主动知识库程序设计语言的途径。重新设计主动知识库程序语言将知识的定义、操作、维护和管理功能与应用程序彻底融合在一起,这自然也是一种可取的途径。这就彻底地解决了所谓"阻抗不匹配"问题。

第一种途径较简单,但效率较差;第二种途径是一折衷的方案,改造的工作量适中,除了在两种语言的接口部分可能损失一定的效率之外,运行效率较好;第三种途径是最彻底的方案,运行效率高,但实现的难度和工作量较大。

3 主动知识库系统在 IDS 中的应用体系结构

3.1 IDS 通用模型

目前尚缺乏 IDS 相应的标准,IETF(Internet Engineering Task Force)和 CIDF(Common Intrusion Detection Framework)两个组织试图对 IDS 进行标准化[4]。CIDF 在 IDES 和 NIDES 的基础上提出了一个通用模型,将 IDS 分为 4 个基本组件:事件产生器、事件分析器、响应单元和事件数据库。如图 2 所示。

在现有的 IDS 中,人们通常用信息获取子系统、分析机

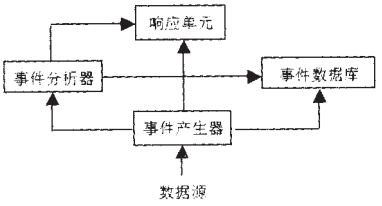

图 2 IDS 通用模型

和响应来替代事件产生器、事件分析器和响应单元。其中,事件数据库用来存放中间数据和检测结果,它可以是复杂的数据库系统,也可以是简单的文本文件。

3.2 体系结构

将主动知识库系统应用于 IDS,除了可以提供所需的检测知识外,还可利用其具有的主动功能提高 IDS 检测效率,且便于对系统的管理。其体系结构如图 3 所示。

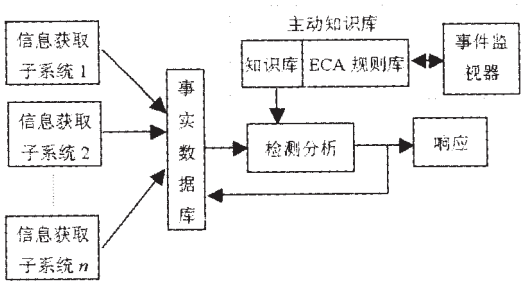

图 3 主动知识库在 IDS 中应用体系

其中,各功能模块作用如下。

(1)信息获取子系统。用来获取所需的各种网络或主机信息,并对这些信息进行过滤,除去那些明显不为入侵的信息。

(2)事实数据库。用来存储各种数据,包括从信息获取子系统获取的数据、分析中间结果、分析结果。

(3)检测分析。依据知识库所提供的知识,对所获取的信息进行分析,以判断其是否为入侵。

(4)主动知识库。主要包括 3 部分:知识库——存储 IDS 所需的检测知识;ECA 规则库——用来存储所制定的 ECA 规则;事件监视器——对系统发生的事件进行实时监视,当所定义的事件发生后,则触发相应的 ECA 规则。

(5)响应。当分析结果为入侵时,响应模块根据入侵方式和入侵级别,采取响应的相应动作。一般分为主动响应和被动响应。

3.3 主动功能

将主动知识库系统应用到 IDS 中,其应具有以下的主动功能。

(1)知识库状态的动态监控功能。对知识库运行状态进行监控,当出现异常情况时,及时报警并自动采取相应的措施。

(2)知识库的自动维护。当知识库中所存储的知识数量增加时,对知识库的一致性、完整性等进行校验,主要包括对知识的矛盾性、冗余性、独立性、相容性和可证明性等方面的校验。

(3)知识库的分块调度功能。当知识库中的知识数量较多时,查找知识则需花费大量的时间,此时,主动知识库可以对这些知识进行分块调度、管理,从而大大提高知识查找

效率。

(4)知识缓冲区内容自动更新功能。在检测分析的同时,主动知识库可以主动从知识库中查找所需的检测知识,并将其放至知识缓冲区中,从而大大提高分析效率。

(5)实现简单的学习功能。由于新的入侵不断出现,因此,知识库中的知识需不断更新。主动知识库系统可以通过其学习功能,发现新的知识,并将其补充到知识库中。

4 检测知识的 ECA 规则表示

当前,大部分入侵检测系统仅仅只关注系统所检测到的原始事件,而忽略了隐藏在这些原始事件背后的逻辑联系和攻击意图。如果这种相关的分析工作全部由系统管理员来人工完成,则工作量巨大且效率低下,最终不仅将严重浪费系统管理员的时间和精力,而且无法实现系统的快速判断和响应。

知识库的主动功能是通过 ECA 规则实现的,而 ECA 规则是由事件驱动继而判断条件是否满足,一旦条件满足,则执行相应的动作。因此,将 ECA 规则用来表示入侵检测知识,不但可以对入侵过程的静态特征进行分析,还可以对由入侵事件相互作用所造成的动态特性进行分析,进而提高入侵检测的分析效率和能力。

4.1 入侵事件特征

入侵过程往往由一系列的入侵行为组成,而每一个入侵行为则包含 1 个或多个入侵事件,同时会在操作系统中产生 1 个或多个事件。从入侵检测的角度来看,入侵事件可以描述为能够引起入侵行为的发生,或具有潜在入侵行为的一切活动、变化和事情。

入侵事件可用如下形式描述[5]。

(1)事件参数声明(Event Name)。

(2)事件参数是指和此事件相关的一些属性,如事件发生的主体、客体和发生时间等。

(3)入侵事件之间的关系主要具有以下特征:存在,即某些事件的出现,就可以充分证明存在攻击的企图;序列,即一系列的事件按特定的顺序发生,便可判断为入侵;部分有序,即几个事件按一定的顺序发生;持续,即一些事件存在或发生的不大于或不小于一定的间隔时间;间隔,即时间的发生有精确的间隔。

4.2 ECA 规则表示检测知识

本文定义以下"4 元组"来描述入侵行为,即事件、系统状态、时间关系、统计关系。

(1)事件:是指由入侵行为所引起的各种事件,既可以是原子事件,又可以是复合事件。

(2)系统状态:是指和事件相关的系统状态,对于网络型事件,系统状态指相关的协议状态。

(3)时间关系:用来表明事件和系统状态与具体时间相关的一些属性,如可以用时间关系来表示事件的持续和间隔关系。

(4)统计关系:是指可以用统计关系来表明的事件和系统状态的一些属性,如对于登录失败事件,如超过 3 次,就可认为有入侵行为发生。

用 ECA 规则来表示入侵行为时,可用 E 来描述事件(原子事件或复合事件),C 来描述系统状态以及相关的时间和统计关系,A 则为当 E、C 都匹配成功后系统所要执行的动作。

用 ECA 表示入侵检测知识有以下两种形式。

(1)EA 规则表示形式。这里默认规则的条件恒为真,说明当某些事件出现后,就可认为有特定的入侵行为发生。

(2)ECA 规则表示形式。当某些事件发生后,并不能确定是否有入侵行为发生,或者不能判断出是哪类入侵行为发生,因此还需对系统状态或者时间关系和统计关系(有时同时包括三者)进行评估,当评估结果为真时才能确定其为入侵行为。

如,对系统登录尝试,当"登录失败"超过 3 次,就可认为有入侵发生。利用产生式规则检测,每次登录时都需要对用户名和密码进行匹配,以判断登录成功与否。而利用 ECA 规则进行检测,只需在系统发生"登录失败"事件后再判断是否已超过 3 次即可,其表示为:

RULE *RuleLog_Failed*
When *Log_failed*(*N*:登录次数)
    If $N \geqslant 3$ Then *alert*;
END RULE

4.3 与产生式规则表示相比较

一般滥用检测方法都缺乏处理序列数据的能力,即无法解决数据前后的相关性问题。产生式规则的条件部分元素之间由于通常以"逻辑与"的关系连接,因此很难准确地检测某些具有时间顺序特点的入侵行为。

如,对于下面两条产生式规则:

r_1:If a & b & c Then *alert*;

r_2:If c & b & a Then *alert*。

其中 a、b、c 为入侵特征。

在专家系统中,r_1 和 r_2 表征的意义相同。当获得的用户行为信息同时满足条件 a、b、c 时,则认为是入侵,并进行报警。由此可见,用产生式表示入侵检测知识,无法体现出入侵特征 a、b、c 出现的先后顺序。

而如果采用 ECA 规则表示检测知识,如:

RULE
When $e_a \cdot e_b \cdot e_c$
    If C Then *alert*;
END RULE

其中 e_a、e_b、e_c 分别为 3 个网络事件,"·" 为事件顺序发生操作符,而用 C 来表示事件发生过程中或发生后一些相关变量属性值。只有当 e_a、e_b、e_c 3 个事件顺序发生,且 C 满足后,才认为有入侵行为发生。

5 总结

本文对主动知识库系统及其实现方式进行了描述,并将其应用到 IDS 中,构建了一个应用模型。利用知识库的主动功能,可以提高 IDS 检测效率并便于对系统管理。同时对入侵事件及其特征进行了描述,并将 ECA 规则机制引入到 IDS 中,分析了被保护系统的动态和静态特性,从而提高了检测性能。本文只是对主动知识库系统在 IDS 中的应用进行了初步研究,如何充分发挥知识库的主动功能以提高 IDS 的功能和性能,还须进一步研究。

参考文献(References)

[1] 何新贵,唐常杰,李霖,等. 特种数据库技术[M]. 北京:科学出

高性能耐火耐候建筑用钢 WGJ510C2 的研制及应用

陈　晓　刘继雄　卜　勇
(武汉钢铁(集团)公司技术中心　　武汉　430080)

〔摘要〕 对武汉钢铁(集团)公司(以下简称武钢)研制的高性能耐火耐候建筑用钢 WGJ510C2 的力学性能、焊接性能、耐火性能、耐候性能及其典型应用进行了研究。试验结果表明:该钢具有优良的综合力学性能,在 600℃温度下的屈服强度均高于其室温下屈服强度的 2/3,完全满足建筑结构用钢耐火安全性的强度许用指标;具有低的焊接冷裂纹敏感性,能承受大线能量(50~100kJ/cm)焊接;裸钢的耐火极限比 Q235 钢高出 44%左右,在考虑建筑设计一级防火标准时,使用该钢可比使用 Q235 钢节省薄型防火涂料 36.5%~50%, 节省厚型防火涂料 26%; 经过 1 800h 加速循环腐蚀以后, 该钢的腐蚀率与 Q235 钢和 Q345 钢相比分别减少 20%和 29%; 经过武汉 10 个月大气曝晒试验的结果也表明, 该钢的耐候性能也明显优于 Q235 钢和 Q345 钢。该钢在大型建筑应用中的实际效果良好。

〔关键词〕 耐火性能　耐候性能　力学性能　焊接性能　大线能量焊接　建筑钢　　〔中图分类号〕 TU511.3
〔文献标识码〕 A　　〔文章编号〕 1000-7857(2005)03-0031-07

INVESTIGATION OF HIGH PROPERTIES FIRE-RESISTANT AND WEATHERING CONSTRUCTION STEEL WGJ510C2 AND ITS TYPICAL USE

CHEN Xiao　LIU Ji-xiong　BU Yong
(NETC of Wuhan Iron & Steel (Group) Corporation, Wuhan 430080, China)

Abstract: The mechanical performance, weldability, fire-resistant, weathering performance and usage of high properties fire-resistant and weathering construction steel developed in Wuhan Steel were evaluated in this paper. It shows that this steel has fine integrated mechanical performance and that the yield strength of the steel at 600℃ is more than 2/3 of the yield strength at room temperature, which is suitable for the fire-resistant safety of constructions. The steel has low cold-cracking sensitivity and can bear high heat input (50~100kJ/cm). The endurance of naked WGJ510C2 is about 44% higher than that of Q235. Considering the fire protection standard Grade One in construction, WGJ510C2 can save 36.5%~50% thin protection coat and 26% thick protection coat, compared with Q235. The result from comparing different steel samples in cyclic corrosion test (CCT) in room and exposed experiment outside (Wuhan, ten months) shows that corrosion speed of new steel (WGJ510C2) is obviously slower than that of traditional construction steel such as Q235 and Q345. The practical use in huge constructions is excellent.

Key Words: fire-resistant, weathering, mechanical performance, weldability, high heat input, construction steel
CLC Number: TU511.3　　**Document Code:** A　　**Article ID:** 1000-7857(2005)03-0031-07

1 前言

钢结构建筑的耐火性能远较砖石结构和钢筋混凝土结构为差。钢材的机械强度是温度的函数[1],一般说来,钢材在高温下的力学性能会发生明显变化, 主要表现在强度和刚度明显降低。温度为 400℃时,钢材的屈服强度降低一半,温度为 600℃时,则基本丧失承载力[2]。钢材在温度升高到某一

收稿日期: 2004-12-28
作者简介: 陈晓,男,1940.5~ ;武汉市冶金大道 28 号武汉钢铁(集团)公司技术中心,副总工程师、教授级高工,主要从事新钢种、新材料的研究与开发; E-mail: chxi@wisco.com.cn

版社,2000,1:85~86
[2] 徐洁磐,马玉书,范明. 知识库系统导论[M]. 北京:科学出版社,2000,1:204
[3] 金光灿.分布式数据库管理系统中主动机制的设计与实现[D]. 华中理工大学学位论文,1996,5
[4] 高峻,吕述望. 入侵检测系统(IDS)[J]. 现代电信科技,2001,9:11
[5] R Sekar, Y Guang, S Verma & T Shanb hag. A high-performance network Intrusion Detection System[A]. In: Conference on Computer and Communications Security, 1999:8~17
[8] 胡昌振. 信息安全的概念及方法论探讨 [J]. 科技导报,2004(3):18~45
(责任编辑　苏　青)