基于 Agent 和 STAT 的入侵检测系统在电力信息系统的研究

董 斌,张少敏,王保义
(华北电力大学 计算机科学与技术学院,河北 保定 071003)

摘要: 首先,分析了电力系统信息网络入侵检测的必要性,然后在状态转移分析 STAT(State Transition Analysis Tool)入侵检测工具的基础上,引入了 Agent 技术,提出了一种基于 Agent 和 STAT 的入侵检测系统。该系统通过 Agent 技术实现了规则更新,并且利用 STAT 技术使该系统可以实时感知入侵状态和进行入侵分析。实验结果表明,基于 Agent 和 STAT 的入侵检测系统能够有效地提高检测率。针对电力系统的特点分析了该系统在其中的应用。

关键词: 入侵检测; 状态转移分析; Agent 技术; 网络安全
中图分类号: TP 393.08 **文献标识码**: A **文章编号**: 1006-6047(2006)01-0037-04

随着人类社会对 Internet 需求的日益增长,网络安全逐渐成为 Internet 及各项网络服务和应用进一步发展所需要解决的关键问题。当前,作为电力自动化系统的数据源和各种控制行为执行者的变电站自动化系统,如果由于网络安全原因引起误动等,将给电力系统的安全带来严重威胁,有时甚至引发灾难性事故。因此,需要一种安全机制来保障网络的安全,入侵检测系统正是这样的一种安全机制。

1 入侵检测系统现状

入侵检测就是通过对系统数据分析,发现非授权的网络访问和攻击行为,然后采取报警、切断入侵线路等对抗措施。入侵检测系统的基本任务是:通过实时检测网络系统状态,判断入侵行为发生,并产生报警。当今的入侵检测系统与各个领域的大量新技术广泛结合,如数据挖掘算法、模糊理论及协议分析技术等。在众多的入侵检测系统所采用的方法中,20 世纪 90 年代在美国加州大学圣巴巴拉分校提出并实现的状态转移分析 STAT(State Transition Analysis Tool)方法[1]由于采用了高层的状态转移表示方法表示攻击过程的策略,从而有效地提高了表示方法的直观性和攻击行为的检测命中率,同时也具备了检测多个攻击者所共同发起的协同攻击及跨越多个进程的攻击行为的能力。然而,由于 STAT 属于给予规则分析的误用入侵检测系统,因此只能检测到已知的攻击类型。本文通过引入 Agent 技术更新事实库,从而使得系统具有更加强大的检测能力。

2 电力信息网络系统的设计与实现

2.1 Agent 技术简介

Agent 是指能在特定的环境下无须人工干预和监

收稿日期:2005-06-22;修回日期:2005-09-07

督完成某项工作的实体。它具有自适应性、智能性和协作性。Agent既能独立地完成自己的工作,又能与其他Agent协作共同完成某项任务,且Agent能够接受控制并能感知环境的变化而影响环境[2]。在一个由多Agent组成的入侵检测系统中,单个Agent的失效只会影响到该Agent和与之协作的部分Agent,系统的其他部分仍能正常工作。如果能将入侵检测系统的功能合理地分配给各个Agent,就能大大减少系统失效的风险,也可以克服传统的使用静态结构的入侵检测系统的许多固有限制[3]。

2.2 入侵检测系统实现

通过对入侵检测系统和Agent技术的分析[4-5],本文提出了基于Agent的STAT入侵检测系统框架如图1所示。它主要由预处理Agent、推理Agent、决策Agent、进化Agent几个模块组成。首先,预处理Agent对审计记录系统中的数据进行处理,根据系统需要提取特征数据;然后推理Agent根据知识库和预处理Agent数据对该行为是否是入侵行为进行判断,如果该行为是一个入侵行为则要判断其进行的状态;决策Agent根据推理Agent的结果向安全管理人员告知并提供相应的辅助决策数据,以便安全管理人员做出响应;安全管理人员根据决策Agent所发出的报告对网络行为采取相应的处理。当系统出现误检或漏检时,安全管理人员向进化Agent发出指令,由进化Agent根据推理Agent对该记录的分析结果对知识库更新。

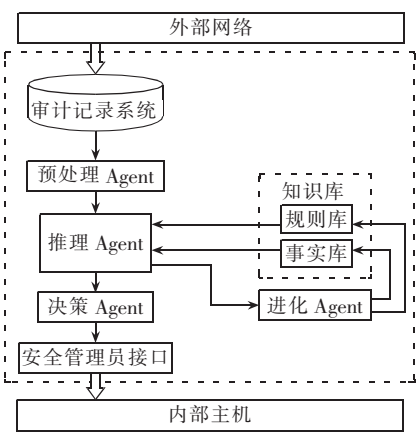

图1 基于Agent和STAT的入侵检测系统框架

Fig.1 Framework of intrusion detection system based on Agent and STAT

2.2.1 预处理Agent

预处理Agent负责对审计记录进行读取、处理和过滤等操作,并将其转化为设定格式后,送交给推理Agent。预处理Agent在对审计记录格式化处理时,负责将审计系统中的事件类型(even type)字段映射到对应的定义好的各个操作类型,如果没有对应操作类型的定义,则丢弃该记录,所有记录失败操作的审计记录也将丢弃。

本模型中所采用的审计记录统一格式由<主体标识、主体访问权限、操作行为、目标标识、目标属主、目标访问权限>6元组定义。

系统针对面向独立的安全审计模块BSM(Base Security Module)审计记录,对不同的目标系统移植时,只要针对性的开发预处理Agent的记录映射模块即可完成格式转化;同时,系统也不需要分析所有的审计事件,而仅仅处理其中的一部分,并将其映射到特定的STAT操作类型上。

2.2.2 推理Agent

推理Agent负责根据知识库(规则库和事实库)的内容,并在预处理Agent数据的基础上,利用STAT技术进行状态推理。推理Agent负责解析规则库中的每条规则,并在所有可用相关知识基础上分析判断,完成入侵检测工作任务。推理Agent采用前向链推理模式,即从输入的事实出发,触发规则最终得出结论。本系统的规则通用表达式如下所示:

$RULE_{i,j}$:State_Description_Table(i,j)

Signature_Action

表达式的具体含义为:若$RULE_{j,i-1}$已经触发,而State_Description_Table(j,i)满足状态断言,则判断特征行为Signature_Action是否发生;若$RULE_{j,i-1}$已经触发,而Signature_Action已经发生,并且随之State_Description_Table$(j,i+1)$满足断言条件,则规则$RULE_{j,i}$触发。

本系统中,通过二维推理表可视化表示推理Agent的工作过程。在推理表中,每一行表示对应的某个具体攻击行为的进行状态,而每一列则表示攻击过程中的某个具体步骤,及这次攻击的完成程度。

2.2.3 决策Agent

决策Agent负责向安全管理人员发送信息,标识当前攻击过程接近完成的程度或者当前攻击是否完成。当检测到某攻击活动即将完成时,则直接采取相应活动,阻止当前的攻击行为。

在决策Agent中引入"决策支持表"表示数据的结果,格式如下所示:(决策i:消息1,消息2,消息3,…);其中存储对应于每个状态转移消息的提示信息和响应建议。当某个状态转移过程完成时,即对应的规则被触发,决策Agent就可根据决策支持表中的相应信息进行不同的响应操作。

决策Agent通常执行的操作有:显示存储在决策支持表中的各种提示信息和响应建议等;显示当前攻击过程中所涉及的所有文件的名称信息;显示执行当前关键操作的用户有效ID号和真实ID号;直接响应阻止攻击行为,如拒绝服务、封锁IP等;

2.2.4 进化Agent

系统知识库由事实库和规则库2部分组成[6]。进化Agent主要负责知识库的更新和事实库的初始化。

事实库是一组文件集合,即一组共同具备某些容易受攻击的属性特征的文件。STAT的文件集合共分为7大类,其中有一类是系统硬连接文件,这个文件

集合中包含了系统中所有连接文件的信息。通过对这个文件集合的定义,使得很多攻击的变种在使用不同文件名调用同一文件时被检测出来。更新事实库是当某些操作所涉及的目标文件类型或某些操作类型变更时,对事实库中的文件集合作相应的调整。其中更新模块主要针对的是连接文件集合和信息,其具体算法为

```
IF AuditRecord implies a HARDLINK action
//记录的操作为创建类型
IF AuditRecord.target is in HardLinks
    {ADD AuditRecord.object to HardLinks
    }
ELSE
    {ADD AuditRecord.object to HardLinks
     ADD AuditRecord.target to HardLinks
    }
ELSE
IF AuditRecord implies a DELETE action
//记录的操作为删除类型,将其从所属文件类型中删除
    IF AuditRecord.object is in Hardlinks
     {DELETE AuditRecord.object from Hardlinks
     }
IF AuditRecord implies a RENAME action
//记录的操作为重命名类型
    IF AuditRecord.obname is in Hardlinks
    {RENAME AuditRecord.obname to Audit
Record.target in Hardlinks
    }
```

规则库中定义了推理 Agent 根据现有事实库和审计记录进行入侵检测分析的步骤。在规则库中,引入状态描述表(state description table)和特征操作表(signature action table)。

在状态描述表中,每一行代表一种攻击活动过程,每一列代表对应每个特定步骤的状态,并且每个状态转移图都对应一组状态断言集合。下面是一个用户越权使用文件的例子:

```
# Unauthorized access to user privileges
#
State_Description-1:
name (file1) ="-* " & not owner(file1) = USER &
permitted
(SUID,file1)
& shell_script(file1) & permitted(XGRP,file1) |
permitted(XOTH,file1).
Not euid=USER
#
```

特征操作表的结构与状态描述表类似,针对每个状态转移图都对应一组特征操作集合。

规则库中每条规则的格式为:〈状态描述表的坐标,记录的操作类型〉

更新规则库:当有某攻击行为未被系统监测到,则由安全人员向进化 Agent 发送该攻击的相关信息,通过与推理 Agent 协作生成新的规则,同时更新状态描述表和特征操作表。

2.2.5　消息 Agent

消息 Agent 负责协同多个主机代理和检测代理共同进行监视。当网络代理发现某个主机有入侵行为时,一方面及时做出反应,如报警或通知此主机上的主机代理,另一方面还可以把情况通知给其他主机上的代理,以提高其他代理的入侵检测能力。

2.3　系统特点

通过对系统各部分的描述,可以发现:由于规则针对操作类型信息存储,所以当规则库中有了一条关于单个 ID 的攻击行为的规则,那么当有多个 ID 分别执行该攻击过程的某些步骤攻击主机时,系统也可以及时地发现该攻击行为[7-8]。例如,规则库中有如下规则:一个攻击者对属主为 root 且具有 setid 特性的 shell 脚本 target,创建一个硬连接文件,并该文件的名称以"-"开头,然后执行该文件就可以获得具有 root 访问权限的 shell。当攻击者 A 以上述方法创建的一个硬连接文件,而由攻击者 B 执行该文件获得 root 访问权限时,这种协同攻击的行为也可以由系统检测出来。因此,系统在检测多用户协同攻击方面具有很大的优势。

3　实验设计与分析

3.1　实验描述

本实验的测试范围是实验室内部局域网,攻击事件是根据 ISS 公司发布的攻击特征参考文档所实施的网络数据包模拟,攻击目标是局域网中的一个主机,涉及的入侵攻击为 Back 攻击、Neptune 攻击、Pod 攻击,他们都属于 DOS 类型攻击。

本实验采用对比法,将一种一般的规则分析检测系统和基于 Agent 和 STAT 技术的入侵检测系统同时运行在服务器上。

实验环境:局域网带宽为 10 Mbit/s,网络主机共 12 台,主机配置为奔腾 4 代 2.4 GHz CPU,512 MB 内存,80 G 硬盘。根据实验需要,通过在局域网内模拟攻击程序,控制攻击次数分别为 100 次、200 次和 300 次,对 DOS 类型攻击实验结果见表 1,2。

表 1　一般规则分析的入侵检测系统实验结果

Tab.1 Test result of IDS based on general rule-analysis

结果	攻击次数		
	100	200	300
检出次数	96	195	292
漏警次数	8	12	20
误警次数	4	7	12

表 2　基于 Agent 和 STAT 的入侵检测系统实验结果

Tab.2 Test result of IDS based on Agent and STAT

结果	攻击次数		
	100	200	300
检出次数	100	199	300
漏警次数	3	2	1
误警次数	3	1	1

通过表1与表2的比较,对DOS攻击随着攻击次数的增加,在检出次数上表2均大于表1,而在漏警和误警次数上却远远小于表1。实验结果表明:基于Agent和STAT技术的入侵检测系统,随着入侵次数的增多,其命中率明显高于一般规则分析入侵检测系统,在漏警率和误警率上明显较低与一般规则分析入侵检测系统。

3.2 入侵检测系统性能分析

基于Agent和STAT技术的入侵检测系统具有下面2点性能。

a. 系统有较高的检测率。由于使用了STAT技术作为入侵检测模型,系统通过对入侵行为的状态进行实时分析和分类,可以准确地检测入侵行为,进而提高了系统检测的检测率。由于规则注重状态分析而不针对某个用户,因此,系统既能够预测攻击行为所带来的隐患,也可以更加准确地检测由多用户协同发起的攻击行为。

b. 系统有较高的灵活性、可扩展性。每一层的Agent都可以由多个Agent完成相应的功能,这样如果某一层的单个Agent由于某种原因停止工作,那么由于各个Agent是互不依赖的并且由它自身产生结果,因此只会丢失它自己的结果,该层的其他Agent可以继续工作,从而提高系统的灵活性和扩展性。

4 结语

从长远的角度考虑,一个强大的体系结构将提高整个安全系统的自适应和进化能力。面对电力系统的安全需求,基于Agent和STAT的入侵检测系统不仅可以及时发现入侵行为和预测入侵行为带来的隐患,而且其灵活性和可扩展性还保证了系统的强壮性。因此,在电力系统中,基于Agent和STAT的入侵检测系统的优势得到了很好发挥。当然,本系统在Agent之间进行通信时,还可以采用数字签名技术和数字证书技术进一步加强系统自身的安全性。相信随着研究的深入本系统将会更加完善。

参考文献:

[1] PORRAS P A. STAT:a state transition analysis tool for intrusion detection[D]. Santa Barbara:University of California,1992.

[2] WEISS G. Multi-agent system,a modern approach to distributed artificial intelligence[M]. Cambridge,MA:The MIT Press,1999.

[3] JANSEN W,MELL P,KARYGIANNIS T,et al. Mobile agents in intrusion detection and response[C/CD]// **Proceedings of the 12th Annual Canadian Information Technology Security Symposium.** Ottawa,Canada:Computer Security Establishment,2000.

[4] 郑文波. 一个基于Agent的IDS结构模型设计[J]. 计算机与网络,2005,3(4):118-119.
ZHENG Wen-bo. A design of IDS model based on Agent [J]. **Computer and Network**,2005,3(4):118-119.

[5] LLGUN K. USTAT:a real-time intrusion detection system for UNIX[D]. Santa Barbara:University of California,1992.

[6] 王勇. 状态网络入侵检测系统的设计和原型实现[D]. 沈阳:东北大学,2002.
WANG Yong. The design and prototype implementation of stateful network intrusion detection system[D]. Shenyang:Northeastern University,2002.

[7] 唐正军. 入侵检测技术导论[M]. 北京:机械工业出版社,2004.

[8] 张勇,冯玉才,李华阳. 基于状态转换分析的多用户入侵检测模型[J]. 网络安全技术与应用,2003(4):50-54.
ZHANG Yong,FENG Yu-cai,LI Hua-yang. Multi-user intrusion detection system based on state transition analysis [J]. **Net Security Technologies and Application**,2003(4):50-54.

(**责任编辑**:汪仪珍)

作者简介:

董 斌(1980-),男,河北唐山人,硕士研究生,研究方向为计算机网络和信息安全(**E-mail**:dbin2000@163.com)。

Research on Agent & STAT-based intrusion detection system of electric power information system

DONG Bin,ZHANG Shao-min,WANG Bao-yi

(School of Computer Science and Engineering,North China Electric Power University,Baoding 071003,China)

Abstract: The necessity of intrusion detection for electric power information network is analyzed and a new intrusion detection system based on both Agent and STAT(State Transition Analysis Tool) is proposed by introducing the Agent-technique. The new system updates rules by Agent-technique,and perceives real-timely the state of intruding activities and analyzes them by STAT. The experimental result indicates that the intrusion detection system based on Agent and STAT is capable of increasing efficiently the detection rate. Its application in electric power system is analyzed.

Key words: intrusion detection; state transition analysis; Agent technique; network security