

基于自律反馈机制的入侵容忍模型

吴庆涛, 华 彬, 郑瑞娟

(河南科技大学 电子信息工程学院, 河南 洛阳 471003)

摘 要: 针对当前入侵容忍系统需要过多人工干预和缺乏自适应性的问题, 提出了一个基于自律计算的容侵系统模型. 该模型借鉴自律计算的思想并引入反馈机制对网络连接的可信度进行实时分析, 生成初始信度, 并通过信度阈值的自主学习与调整实施动态的信度优化, 实现对可疑连接的自律容忍.

关键词: 自律计算; 反馈控制; 入侵容忍

中图分类号: TP393.08

文献标识码: A

文章编号: 1000-7180(2011)04-0099-04

Intrusion Tolerance Model Based on Autonomic Feedback Mechanism

WU Qing-tao, HUA Bin, ZHENG Rui-juan

(Electronic & Information Engineering College,
Henan University of Science & Technology, Luoyang 471003, China)

Abstract: According to the problem that the current intrusion tolerance system requires too much manual intervention and lack of self-adaptability, this paper proposes a model of intrusion tolerance system based on autonomic computing. The model drawing on autonomic computing ideas and feedback mechanism can analyze the reliability of the network connection in real time and generate initial reliability, and though the reliability threshold's independent study and adjustment, implement the dynamic reliability optimization, and ultimately tolerate the suspicious connections, achieve the goal of protecting the target system security.

Key words: autonomic computing; feedback control; intrusion tolerance

1 引言

由于网络系统的安全威胁和潜在风险层出不穷、无处不在. 传统信息安全技术面对随时可能出现的随机事样显得无能为力, 人们期望有一种自动、灵活、细粒度的方法来解决系统可生存性问题, 其中入侵容忍技术是系统可生存技术的核心. 入侵容忍技术强调当系统的某些部分已经受到破坏, 或者已经受到攻击者的控制时, 整个系统仍然能够继续对外提供服务, 并保证数据的保密性、可用性和完整性.

近些年来, 借助于自律思想, 希望系统能够自治运行并自我调整以适应不同的环境, 解决系统的容

侵问题. 文献[1]从资源分类控制的角度建立了一种并行容侵系统研究模型—RC(Resource Control)模型, 并给出了实例分析; 文献[2]提出了一个优化的系统状态转移模型, 用以描述具有自我演进能力的入侵容忍系统的动态行为, 通过计算模型中时间参数敏感度, 得出了入侵容忍技术研究的关键点; 文献[3]提出了一个基于自律计算的自适应分级入侵容忍系统模型^[4], 该模型主要由信度评估、服务分级、诱骗机制、执行模块四部分组成. 这些模型大都是框架上的模型, 对于如何根据系统当前状态、安全性以及内外部环境参数等的变化情况, 对容忍入侵系统的配置和相应运行参数进行动态调整以及如何调

收稿日期: 2010-03-23; **修回日期:** 2010-06-03

基金项目: 国家自然科学基金项目(61003035); 河南省教育厅自然科学研究项目(2009A520012); 河南省高校青年骨干教师资助计划(教高[2009]844号)

整,则很少涉及。

本文将自律计算的思想引入入侵容忍系统的设计与建模中,并结合了反馈控制的机制,构建了一个容侵系统模型,该模型能够对系统内外部参数进行监视,分析并及时动态调整系统中的参数,增强了系统自适应能力和可用性。

2 自律反馈机制

自律计算的思想来源于人体自律神经系统,自律计算是指根据系统的内外需求变化动态地、主动地调整软硬件资源来管理自身的能力,是一种实现系统管理的新方法、新思路,其目的在于实现自我管理,以最少的人工干预完成系统的自配置、自修复、自优化和自保护,从而降低复杂计算环境下的管理成本,提高系统的可用性。

2001 年 IBM 提出了“自律计算”的概念,它一经提出就受到了世界著名 IT 公司和科研机构的广泛关注,如微软的“可信赖计算”、惠普(HP)的“自适应计算”等。浙江大学廖备水等在阐述自律计算概念的基础上,提出一个自律计算的概念模型^[5],该模型刻画了自律元素和自律计算系统的基本工作机制和原理。自律计算系统由若干相互联系的自律元素组成,自律元素又由自律管理者(Autonomic Manager, AM)和被管资源(Managed Resource, MR)组成,如图 1 所示。ACS 在策略的指导下,这些自律元素在实现内部自适应的同时,通过交互协作实现整个系统的自适应。

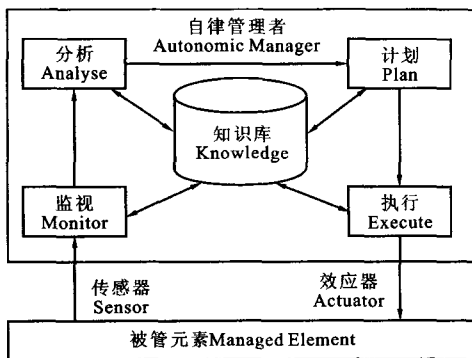


图 1 自律元素构成图

2.1 自律管理者工作机制

AM 的基本工作机制可以表示为图 2。策略知识集合 K_p 包含三类策略:动作策略(P_A)、目标策略(P_G)和效用函数策略(P_U)。动作策略和目标策略表示为:IF $v(s_i, s_c)$ THEN δ 。式子中 $s_i \in S_i, s_c \in S_c$ 分别是当前的内部状态和上下文状态;评估函数 $v(s_i, s_c)$ 依据当前状态决定策略是否被执行。 δ 是该

策略的反映方案。

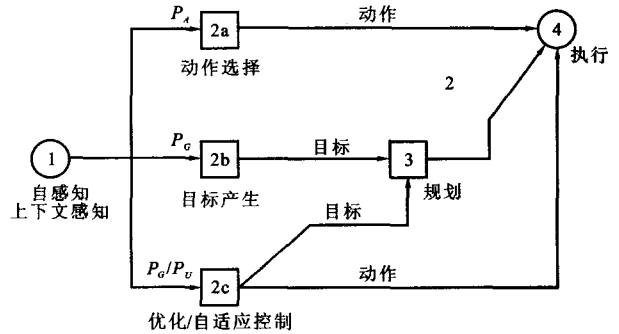


图 2 自律管理者工作机制

AM 工作机制主要由四个步骤组成:1、自我觉察/上下文觉察;2、基于策略的决策;3、目标导向规划;4、动作执行。根据不同的问题域和自主管理的目标,每个控制循环有不同的工作机制。

- (1) 1→2a→4;
- (2) 1→2b→3→4;
- (3) 1→2c→3→4;
- (4) 1→2c→4

在上述四个机制中,第一个步骤是自我觉察、上下文觉察,它是 AM 进行决策的依据。第二个步骤是基于策略的决策,它是 AM 的核心部分,依据策略的不同可以分为 3 种不同的决策过程:(2a)动作选择(Action Selection):使用的策略为动作策略,这时 δ 是可执行动作,当 $v(s_i, s_c)$ 为真时,如果不存在冲突,则被选择,直接输出结果;(2b)目标产生(Goal Generation):使用的策略是目标策略,这时 δ 是抽象目标,当 $v(s_i, s_c)$ 为真时,如果不存在冲突,则被选择为目标并送往规划部件;(2c)优化/自适应控制(Optimization/Adaptive Control):使用的策略为效用函数策略或者目标策略,此时的目标策略一般是期望的系统性能指标,对于效用函数策略,AM 通过计算系统的最大效用值来确定最优的反映方案。第三和第四个步骤分别是规划和执行。

2.2 自律管理者组织结构

在一个自律计算系统中,参与协作的自律管理者以一定的方式形成组织,以便提供系统级的自律管理功能。AM 组织结构研究个体 AM 之间的信息和控制关系模式,自律管理者的对等组织结构如图 3 所示。在 AM 组织结构中,包含三个基本要素:自律管理者、AM 之间状态信息传递关系(state information, SI)和控制信息传递关系(control information, CI)。AM 的组织结构定义为 3 元组 $G=(M, S, C)$,式子中 M 是所有 AM 的集合, S 是 SI 的集合, C

给网络可信度评估模块. 系统评估的内容主要有: 系统安全性评估、系统可靠性评估、系统可维度评估等量指标. 通过自律管理者使系统的可信度维持在一个稳定的范围内.

3.4 反馈调节机制

两个自律元素之间的信息交互, 是整个系统运行及参数自主调节的关键. 当系统安全性评估的结果偏低, 而网络连接可信度评估结果相对较高时表明把攻击信息误判为可疑信息的比例高, 需要增大可疑信息区间的下确界. 当系统安全性评估的结果偏高, 而网络连接可信度评估结果相对较低时表明把可信信息误判为可疑信息的比例高, 需要减小可疑信息区间的上确界. 系统平稳运行的时候, 安全性评估曲线与网络连接可信度评估曲线应基本相一致, 如果差别过大时就需要对可信度阈值进行调节, 其调节过程可以用图 6 来模拟.

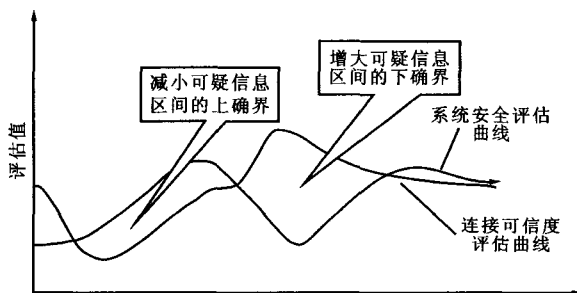


图 6 阈值调节过程示意图

4 结束语

本文借鉴了自律计算的思想以及自动控制中的

反馈的机制, 构建了一个入侵容忍系统模型, 具备较好的自适应性, 能动态调整各个子模块的运行参数, 使系统对已知和未知的攻击具有容忍能力.

将自律计算与入侵容忍相结合的研究还处于起步阶段, 相关的方法和理论还需要进一步的研究和完善. 计算机系统评估技术在此模型中也起到了关键的作用, 计算机系统评估技术与传统的入侵容忍技术相结合将是一个很好的研究方向.

参考文献:

- [1] 崔竞松, 王丽娜, 张焕国. 一种并行容侵系统研究模型—RC 模型[J]. 计算机学报, 2004, 27(4): 500—506.
- [2] 殷丽华, 方滨兴. 入侵容忍系统安全属性分析[J]. 计算机学报, 2006, 29(8): 1505—1512.
- [3] 李冰洋, 王慧强. 自律入侵容忍系统的模型构建与量化分析[J]. 计算机应用研究, 2009, 26(5): 1883—1886.
- [4] 邓林, 余刘琅. 基于入侵容忍原理的服务器防护技术[J]. 微电子学与计算机, 2008, 25(6): 143—146.
- [5] 廖备水, 李石坚. 自主计算概念模型与实现方法[J]. 软件学报, 2008, 19(4): 779—802.

作者简介:

吴庆涛 男, (1975—), 博士, 副教授, 硕士生导师. 研究方向为网络信息安全.

华彬 男, (1983—), 硕士研究生. 研究方向为网络安全.

郑瑞娟 女, (1980—), 博士, 讲师. 研究方向为网络信息安全、可信计算.

(上第 98 页)

- [4] Moses Liskov, Ronald L Rivest, David Wagner. Tweakeable Block Ciphers[C]// CRYPTO 2002, LNCS 2442, 2002. Berlin Heidelberg: Springer—Verlag, 2002: 31—46.
- [5] 王海洋, 陈弘毅. 一种小面积的高吞吐率 AES 协处理器设计[J]. 微电子学与计算机, 2009, 26(6): 12—16.
- [6] 余国义, 李皓, 刘国希, 等. 一种适用于 DSP 的安全模块的设计[J]. 微电子学与计算机, 2009, 26(7): 1—4.
- [7] 华漫. AES 算法分析及其硬件实现设计[D]. 成都: 西南交通大学, 2004: 36—38.

- [8] 卢坚. 高级加密标准研究及其 FPGA 实现[D]. 成都: 西南交通大学, 2002: 41—44.

作者简介:

李子磊 男, (1985—), 硕士研究生. 研究方向为信息安全、数字 IC 设计.

刘政林 男, (1968—), 教授. 研究方向为集成电路设计、无线传感器网络、嵌入式系统安全等.