

一种具有自律特征的入侵容忍系统模型

刘 彬^{1,2}, 吴庆涛¹, 郑瑞娟¹

(1 河南科技大学 电子信息工程学院, 河南 洛阳 471003; 2 河南省汝南园林学校 计算机系, 河南 驻马店 463300)

摘 要: 针对当前入侵容忍系统缺乏自律性的问题, 提出一种基于自律计算的入侵容忍系统模型. 系统模型关键模块涵盖了入侵行为的检测评估、自律管理者的自主学习与自律容侵中心的容侵措施; 同时通过检测评估中心构建进程危险函数, 产生入侵行为的危险函数值, 由自律管理者动态比较和调整危险函数值与入侵阈值的关系, 实现了对入侵行为的自律容忍. 最后通过实验分析了系统对入侵行为的自律容侵过程.

关键词: 入侵容忍; 自律计算; 危险函数; BP 神经网络

中图分类号: TP393

文献标识码: A

文章编号: 1000-7180(2012)07-0167-04

Autonomic Intrusion Tolerance System Model

LIU Bin^{1,2}, WU Qing-tao¹, ZHENG Rui-juan¹

(1 Electronic & Information Engineering College, Henan University of Science & Technology, Luoyang 471003, China;
2 Computer Department, Runan Garden School, Zhumadian 463300, China)

Abstract: Aiming at the absence of autonomic on existent intrusion tolerance system, this paper proposed an intrusion tolerance system model based on autonomic computing. The critical models included detection evaluation of intrusion, autonomic learning of autonomic manager and intrusion tactics of autonomic intrusion centre; and construct danger function of intrusion process, and generate the danger function value of intrusion, the autonomic manager compare or adjust the danger function value and intrusion threshold, dynamic to take appropriate intrusion measures. Finally, the experimentation is given to explain the autonomic intrusion tolerance.

Key words: intrusion tolerance; autonomic computing; danger function; BP neural network

1 引言

入侵容忍的相关概念早在 1982 年已被提出^[1-2]. 90 年代初期, 国外已开发了具有容忍功能的分布式计算机系统, 主要研究计划包括由美国国防部资助的 OASIS(Organically Assured and Survivable Information Systems)计划和由欧洲 IST(Information Society Technologies)开启的 MAFTIA(Malicious and Accidental-Fault Tolerance for Internet Applications)计划^[3]. 国内对入侵容忍技术的研究相对比较晚. 文献[4]研究了入侵容忍原理的服务器防护技术, 并对入侵容忍模式下的防护效果

评估问题进行了原则性分类. 文献[5]提出了一个具有入侵容忍特性的 Web 服务器系统, 应用了多代理、多样性和冗余等入侵容忍技术. 文献[6]针对入侵行为破坏系统安全性的问题, 提出了资源型安全的概念, 达到了入侵容忍的目的.

目前的研究思路比较局限, 在技术实现上缺乏自律特征, 这使得现有的容侵系统不具备动态自律容忍的功能^[7]. IBM 公司提出自律计算的构想, 由自律计算机制所构建的系统应具备四个主要特征, 即自配置、自修复、自优化和自保护^[8-9]. 文中提出将自律计算技术应用于入侵容忍系统研究中的思想, 给出一种具有自律特征的入侵容忍系统模型, 以实

收稿日期: 2011-10-08; **修回日期:** 2011-11-09

基金项目: 国家自然科学基金项目(61003035); 河南省高等学校青年骨干教师资助计划项目(2009GGJS-050); 河南省教育厅自然科学研究计划项目(2010A520018)

现系统的自我保护。

2 自律入侵容忍系统模型结构

系统模型在结构上借鉴自律计算系统的工作机制,在现有入侵容忍系统模型的基础上,增加并设计了自律管理者、自律检测评估中心和自律容侵中心等模块,并将自律元素融入到各关键功能模块中,如图 1 所示。

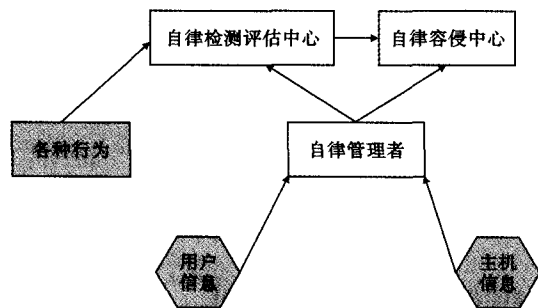


图 1 自律容侵系统核心模块结构

其中,自律管理者负责收集内外部信息并进行分析判断以确定系统的行为;自律检测评估中心负责收集各种进程,实现对进程的监控和评估;自律容侵中心则根据自律检测评估中心的评估及响应的结果采取相应的容侵措施。

2.1 自律管理者

自律管理者由监控、分析、计划和执行,以及传感器、效应器和知识库等部件构成,如图 2 所示。其中,监控和分析部件提供自我觉察和外部环境觉察的能力,并以此为基础进行自主决策,确定系统的自律目标。计划和执行部件实现系统状态偏离期望目标时的自律功能。上述四个功能部件均在知识库的支持下自主学习运作。传感器具有收集组件状态和状态迁移信息的机制。效应器具有改变组件状态配置的功能。

自律管理者的主要工作是收集用户信息和主机

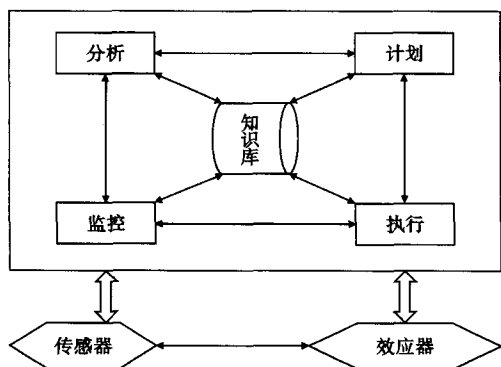


图 2 自律管理者

信息,并监控反馈自律检测评估中心和自律容侵中心的运行状态,来进行综合分析判断以确定系统的行为。

2.2 自律检测评估中心

该中心主要包括进程截获模块、异常检测模块、可疑评估模块和自律模型产生模块等,如图 3 所示。

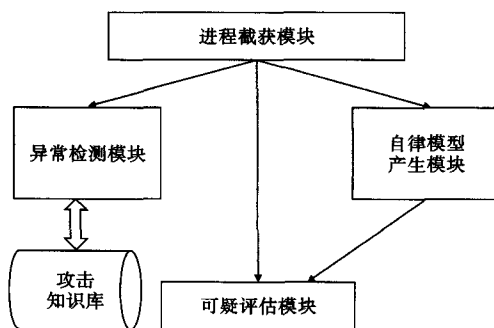


图 3 自律检测评估中心

进程截获模块监听截获实时进程,然后将进程送至异常检测模块。异常检测模块依据攻击知识库对该进程进行异常检测。由于异常检测对未知形态或还未形成的入侵无能为力,因此,在对进程异常检测的同时对该进程进行可疑评估。

(1) 可疑评估的方法

由于入侵行为的诸多不确定性,从概率上对进程进行可疑评估判断。将进程分为三种类型:正常进程、可疑进程和入侵进程。而对于每一个运行的进程,采用概率的方法得出该进程对应于上述每一种进程类型的概率值,然后将得出的概率值代入危险函数,求出该进程相应的危险函数值。

设进程 T 对应于正常进程的概率值为 P_n ,对应于可疑进程的概率值为 P_s ,对应于入侵进程的概率值为 P_i ,则进程 T 的危险函数为

$$f(t) = K_n P_n + K_s P_s + K_i P_i \quad (1)$$

$$(K_n \geq 0, K_s \geq 0, K_i \geq 0)$$

式中, K_n 、 K_s 、 K_i 为权系数,用于调整不同进程的类型对危险函数值的影响程度,权系数可以根据经验或评估技术确定。

(2) 可疑评估的步骤

① 进程截获模块监听截获网络数据进程并记录进程的状态,然后将进程及其状态同时发送至自律模型产生模块和可疑评估模块。

② 自律模型产生模块通过自律管理者发送来的信息,在现有检测模型的基础上,通过自主学习产生新的检测模型,并将新产生的模型送至可疑评估模块。

③ 可疑评估模块接收自律模型产生模块产生

的新检测模型并更新现有检测模型,同时利用检测模型对传来的进程实施可疑评估,一旦检测到可疑进程,通过进程危险函数计算危险函数值,并产生可疑信息,然后将可疑信息发送至自律容侵中心。

2.3 自律容侵中心

该中心主要包括可疑信息接收分析模块、自容忍措施、自恢复措施和自销毁措施等模块。如图4所示。且各模块都受自律管理者的支配和调节。其中,自容忍措施包括提供服务、降级服务和拒绝服务;自恢复措施是在自律管理者的自律反馈控制结构指导下采用微重启或热插拔的技术;自销毁措施采取的是销毁系统部分或全部内容的方法。

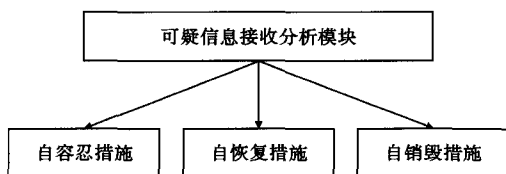


图4 自律容侵中心

可疑信息接收分析模块接收来自自律检测评估中心的可疑信息,分析其中的危险函数值,并将危险函数值与入侵阈值相比较,如图5所示。

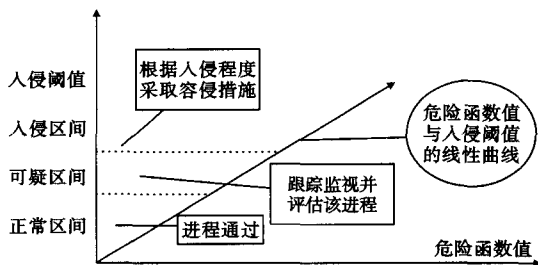


图5 危险函数值与入侵阈值的关系

这里定义进程入侵阈值为 Y ,其与进程危险函数 $f(t)$ 成线性关系:

$$Y = R \cdot f(t) \quad (2)$$

$$\text{即 } Y = R(K_n P_n + K_s P_s + K_i P_i) \quad (3)$$

式中, R 为修正权系数,用于调整危险函数与入侵阈值的关系。

当危险函数值与入侵阈值比较后,得出相应进程的可疑特征:正常进程、可疑进程或入侵进程。并根据进程的可疑特征采取相应的容侵措施。

具体容侵过程:

(1) 危险函数值与入侵阈值比较后,一方面,将进程可疑状况加入自律管理者的知识库中,以便自律学习,另一方面,若判断进程是正常进程时不需容忍,进程通过;若判断进程是可疑进程时,转入步骤②;若判断进程是入侵进程时,转入步骤③;

(2) 在自律管理者的监控下,由自律检测评估中心继续检测此进程,并实时进行可疑评估,并把可疑评估信息发送至可疑信息接收分析模块,然后进入步骤①;

(3) 根据该入侵进程的危险程度采取相应的容侵措施。具体过程是:当判断到进程是入侵时,进行不间断检测,判断该入侵是否威胁到系统的核心功能模块,若是则采取自销毁措施,否则调用相应的自容忍措施进行容忍,若不能容忍或容忍失败时,将采用自恢复措施进行自恢复。

3 实验及分析

系统实现的关键是能够自律容忍入侵,因此实验的核心部分是系统怎样动态地采取相应的容侵措施,这就需要实验分析危险函数值与入侵阈值的关系,以动态自律地确定系统的容侵行为。由此,采用BP(Back Propagation)神经网络对记录进行可靠度评估,来计算危险函数值。

实验PC机的硬件配置是Intel Pentium 双核CPU,主频为2.0 GHz,内存1 GB,软件环境是在Windows XP操作系统下,用MATLAB7.0进行仿真。从KDD cup99数据集中选取21条记录作为训练集,设其可靠度评估值为 P ,相对于正常数据记录,用接近1的数作为期望评估值,相对于入侵数据记录,用接近0的数作为期望评估值。而危险函数的权系数 K_n, K_s, K_i 分别设为0.2, 0.5, 0.8。其进程相对于正常进程的概率,用 $P-0.2$ 的绝对值作为概率估值 P_n ,相对于可疑进程的概率,用 $P-0.5$ 的绝对值作为概率估值 P_s ,相对于入侵进程的概率,用 $P-0.8$ 的绝对值作为概率估值 P_i 。由于系统输出值的范围在 $[0, 1]$ 之间,故BP神经网络输出层的传递函数采用S型对数函数,隐含层传递函数采用S型正切函数,训练方法采用L-M优化算法。由此得出21条记录可靠度,仿真结果如图6所示。

为了便于计算和分析,从仿真图中选择10条记录,统计出其对应的 P 值,由此计算出相应的 P_n, P_s 和 P_i 值,并通过公式(1)和(3)计算出危险函数 $f(t)$ 的值和 Y 的值。如表1所示。

定义区间 $(0, 0.3)$ 为正常区间,区间 $(0.3, 0.5)$ 为可疑区间,区间 $(0.5, 1)$ 为入侵区间。当 $R=1$ 时,将这10条记录的入侵阈值 Y 分别与各区间对比可得出,记录3, 9, 10是正常信息,记录6, 15, 18, 19是可疑信息,记录12, 16, 21是入侵信息。这些记录信息被自律管理者收集并发送到自律容侵中心,自律

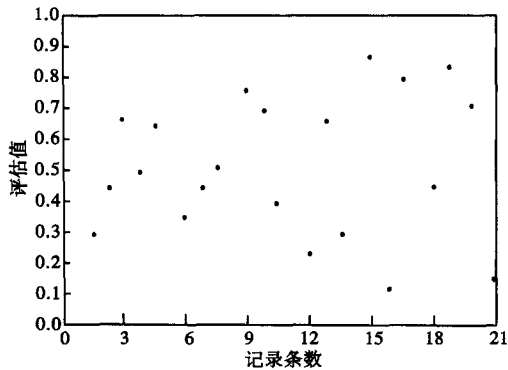


图6 记录可靠度仿真结果

表1 运行结果统计表

记录	3	6	9	10	12
P	0.65	0.34	0.76	0.68	0.25
$f(t)$	0.29	0.48	0.27	0.28	0.58
$Y_{R=1}$	0.29	0.48	0.27	0.28	0.58
$Y_{R=1.2}$	0.34	0.58	0.31	0.34	0.69
记录	15	16	18	19	21
P	0.88	0.12	0.45	0.85	0.15
$f(t)$	0.39	0.75	0.36	0.35	0.71
$Y_{R=1}$	0.39	0.75	0.36	0.35	0.71
$Y_{R=1.2}$	0.47	0.90	0.43	0.41	0.85

容侵中心将按照以上的容侵过程自律地采取相应的容侵措施。

如果此时主机系统还出现入侵行为,这说明危险函数值与入侵阈值的线性调节关系存在不足,容侵系统将一些入侵信息看成是可疑信息或正常信息。这时自律管理者通过收集系统的相关信息来发出相应的指令,动态自律地调整修正权系数 R 的值,如将 R 值设为 1.2,来增大 Y 值。由此,可得出相应记录的可疑特征,记录 3,9,10,15,18,19 是可疑信息,记录 6,12,16,21 是入侵信息,这时发现了更多的可疑信息和入侵信息,并做出相应的处理。

然而, R 值太大,会将一些正常信息误认为是入侵信息; R 值太小,会将一些入侵信息看成是正常信息。因此, R 值应由自律管理者收集系统的内外部信息动态自律地调整确定。

4 结束语

本文借鉴自律计算的思想,构建了一个自律入侵容忍系统模型,并对其中的关键功能模块进行了详细设计。该系统模型能够由自律管理者模块收集系统内外部信息,并进行自律学习,以此动态地调整关键功能模块的运行参数,并采取相应的容侵措施,实现对入侵行为的自律容忍。下一步研究的方向是:

如何确立自律容侵系统的容忍指标,并从可生存性角度研究自律容侵系统的安全态势。

参考文献:

- [1] 孙钦东,刘遵雄,张德运. 网络入侵防御技术研究[J]. 微电子学与计算机,2004,21(7):45-47.
- [2] 张云英,努尔布力,王程明,等. 入侵容忍综述[J]. 吉林大学学报:信息科学版,2009,27(4):389-394.
- [3] Organically assured and survivable information system (OASIS) [EB/OL]. [2010-01-02]. <http://www.all-acronyms.com/cat/2/OASIS/>.
- [4] 邓林,余刘琅,韩江洪. 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] 黄建华,夏亚敏. 入侵容忍技术在 Web 服务器系统的应用[J]. 计算机应用与软件,2008,25(3):252-258.
- [6] 周华,孟相如,张立等. 分布式入侵容忍系统的主动恢复算法研究[J]. 西安电子科技大学:自然科学版,2009,36(2):378-383.
- [7] 王晓静,张晋. 自主计算研究综述[J]. 辽宁大学学报:自然科学版,2010,37(3):214-216.
- [8] 马会彬,赵晓南,李战怀. 具有自律特征的网络故障管理框架[J]. 微电子学与计算机,2006,23(6):49-52.
- [9] 刘文洁,李战怀. 一种基于自律计算的性能监视工具[J]. 微电子学与计算机,2008,25(3):131-133.

作者简介:



刘彬 男,(1981—),硕士研究生. 研究方向为网络信息安全、入侵容忍。



吴庆涛 男,(1975—),博士,副教授. 研究方向为网络信息安全、入侵容忍、可信计算。



郑瑞娟 女,(1980—),博士,副教授. 研究方向为网络信息安全、入侵容忍、自律计算。