

基于生物免疫原理的生存网络系统 SuNSIA 设计

李红英 谢小权

(中国航天科工集团二院 706 所 北京 100854)

〔摘要〕 网络系统生存性是当前的研究热点之一,但目前仍缺乏公认的生存网络系统构建方法或评估网络系统生存能力的方法。结合自然界生物(如人自身)和生存网络系统之间的相似性,提出了一个基于生物免疫原理的生存网络系统(SuNSIA),描述了 SuNSIA 的体系结构、主要模块及工作流程,并分析了 SuNSIA 的优缺点。

〔关键词〕 生存性 生物免疫系统 网络安全 〔中图分类号〕 TP393.08

〔文献标识码〕 A 〔文章编号〕 1000-7857(2005)04-0013-03

SURVIVABLE NETWORK SYSTEM: AN IMMUNOLOGICAL APPROACH

LI Hong-ying XIE Xiao-quan

(Institute 706, The Second Academy of China Aerospace Science and Industry Corp, Beijing 100854, China)

Abstract: The survivability of the network system is increasingly drawn high attention, but a well-accepted construction or evaluation method is still lacking for it. Based on the similarity between survivable network system and natural beings (e.g. human self), a survivable network system based on biological immune system, SuNSIA was proposed, and its architecture, main module and work flow were described. Finally, the advantages and disadvantages of SuNSIA were analyzed.

Key Words: survivability, biological immune system, network security

CLC Number: TP393.08

Document Code: A

Article ID: 1000-7857(2005)04-0013-03

1 引言

信息安全越来越引起人们的关注,但是通过加固实现防护的传统安全观念使得计算机安全成为一种二值的概念:任一给定时刻,系统要么是安全的,要么就是不安全的。惨痛的教训一次次告诉人们,任何现实可行的系统都不可能都是绝对安全的。生存性不同于传统安全技术,它承认系统可能而且会受到攻击等意外事件的影响。基于这种假设,生存性强调系统在攻击、失效、自然灾害等意外事件发生时及时完成任务的能力^[1]。生存性研究正处于起步阶段,目前尚无公认、成熟的生存网络系统构建方法,缺乏有效的网络系统生存能力评估方法。

本文根据自然界生物(如人自身)和生存网络系统之间的相似性,提出了一个基于生物免疫原理的生存网络系统——SuNSIA(Survivable Network System: an Immunological Approach)。

2 生物免疫系统概述

自然界生物处于动态变化的恶劣环境中,经常会受到组织破坏、自然灾害和各种病原体的威胁,不能够适应这种外部环境的生物就会灭亡。因此,经过长期进化的自然界生物自身就存在一个健壮的生存系统,免疫系统是生物最主要的保障体系。下面给予简要介绍,更详细的内容可参见参

考文献。

免疫系统是生物多层次的体系结构,最基本的是皮肤和由 pH 值与体温构成的生理屏障,接下来是固有(innate)免疫系统和适应性(adaptive)免疫系统。固有免疫是种系发育和进化过程中形成的免疫防御功能,因而是不变的,并且识别病原的能力还会受到种系发育和进化过程的影响。适应性免疫中的淋巴细胞则通过学习能够识别未知病原,从而能提供一种通用的防护,并能保留对该病原的记忆以防止同一病原再次的感染。在组织结构上,免疫系统以组织或器官为单位,划分成相对独立的部分,这就防止了一个组织或器官感染而造成机体整体死亡^[2-4]。

网络系统与生物免疫系统有诸多类似之处,因此可以借鉴生物免疫系统的结构体系作为生存网络系统构建的指导准则。

3 设计思想

通过对自然界生物保障体系中一些增强系统健壮性的优良机制和特性的模拟,构建了 SuNSIA,希望通过对这些优良机制的模拟,SuNSIA 能够解决现有生存网络系统构建中存在的一些问题,增强系统在恶劣环境下的健壮性,满足网络系统生存性要求。

SuNSIA 主要基于以下两个方面进行模拟:一是系统的

收稿日期:2005-03-01

作者简介:李红英,男,1978~;北京市 142 信箱 406 分箱 4 号中国航天科工集团二院 706 所,主要从事网络安全研究;E-mail:

occult_xiaoyi@yahoo.com.cn

管理控制结构,将中、小规模局域网络看作生物体的组织或器官,按照组织内部和组织之间的交互原则进行局域网内部和局域网之间的交互。按照免疫系统的结构特点,一个组织的行为应该趋向于局部化,这种分布性和自治从管理的角度增强了系统的健壮性。另一方面就是系统面对病原体入侵或组织破坏时的动态响应行为。在系统遭受攻击或破坏时,首先通过检测识别这些意外事件,通过将检测报警信息归类、融合、关联,不仅能对当前所处攻击的状态有一个整体的把握,并且还能够容忍一定程度上检测系统的漏报。通过模拟免疫系统的协同刺激,对报警信息进行校验来清除误报,从而使系统能够容忍一定程度的误报。对于检测到的已知攻击,根据攻击和系统状态信息快速地做出响应。检测到未知攻击时,则还要通过提取攻击签名的方法进行学习,满足系统适应未知攻击的能力。

4 体系结构

如前所述,SuNSIA 主要是基于对生物免疫系统的模拟。表1给出了生物免疫系统和 SuNSIA 之间功能的映射。

表1 免疫系统和 SuNSIA 之间功能的映射

免疫系统	SuNSIA
隔离、抑制病原	使用防火墙、加密等措施阻断针对系统的攻击;提供不适合某些攻击的网络环境
检测病原	通过入侵检测、病毒检测、QoS 监控等检测系统中的攻击、入侵、应用服务损坏
抑制感染	通过各种措施控制攻击影响的范围,防止攻击在整个系统中的蔓延
协同刺激	对一些检测单元(如异常检测)发出的报警信息进行校验,清除报警信息中的误报
适应	学习、识别未知攻击
免疫记忆	由前面对未知攻击的学习识别,提取出的未知攻击签名
病原清除	阻断、清除系统中检测到的攻击
再生(恢复)	对系统中受损的服务进行恢复,服务恢复方式可以是重新启动服务程序,也可以是恢复到预先设置的一个检测点

把表1中的各功能对应到实在的模块中,得到 SuNSIA 体系结构,如图1所示。图中上方的椭圆表示被保护网络系统,椭圆中的小圆代表被保护网络系统中的各个主机,执行模块和探测器都位于主机内部,被保护网络下面的各椭圆是 SuNSIA 体系结构中的模块,箭头的方向表明了体系结构中各部分之间的信息交互。SuNSIA 体系结构中共包括7个模块,下面分别进行说明。

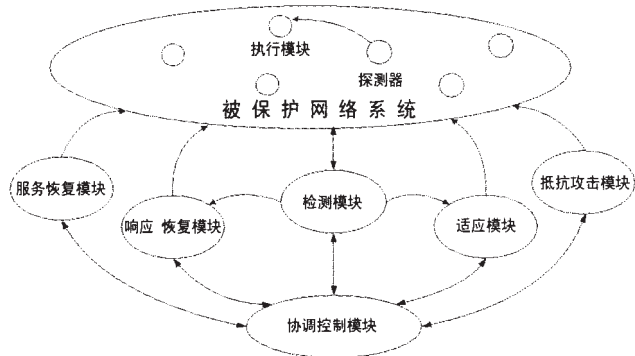


图1 SuNSIA 体系结构

(1)抵抗攻击模块:通过设置屏障将攻击与网络系统隔离开,这一部分对付了绝大多数的攻击。

(2)检测模块:检测针对系统的攻击行为(包括入侵)、应用服务破坏,并发出报警,整个系统动态行为是由检测模块驱动的。

(3)适应模块:对系统中新的攻击进行学习识别,自动生成补丁程序或者可以用于过滤该种新的攻击及其简单变种的攻击签名,从而提高系统的柔韧性和灵活性。

(4)执行模块:响应和修复策略的具体执行单元,包括对攻击的控制、阻断、清除及其影响的修复。

(5)服务恢复模块:恢复系统中受损的服务,包括攻击进行中及攻击完成后的恢复,它属于响应的一部分。

(6)响应和修复模块:结合攻击和系统状态信息生成响应和修复策略。

(7)协调控制模块:协调系统中各个单元,保证系统中的各种机制能够高效地协作。

5 系统工作流程

如图2所示,首先是防护模块阻断了绝大多数攻击。对于成功穿越了防护系统的攻击,系统中有位于主机层和网络层的检测系统对其检测,各个检测单元生成的报警信息经过预处理、归类、融合后生成代表该攻击的一个新的报警信息。按照攻击类型的不同,系统接下来的处理也不相同。对于已知攻击,响应和恢复模块根据攻击描述信息和系统当前状态快速生成响应和修复策略,然后交由执行模块具体执行该响应和修复策略。未知攻击的处理相对较复杂。异常检测系统检测到异常信息,通过延迟等控制措施尽量减小攻击影响的范围。报警校验对报警信息的正确性进行检查,对于误报,执行单元撤销控制,而对于报警校验确认的未知攻击,则会引发适应模块对于新的攻击的学习、生成、优化新识别攻击的过滤规则,从而还可以过滤新识别攻击的简单变种。接下来同样要对攻击造成的影响进行修复。

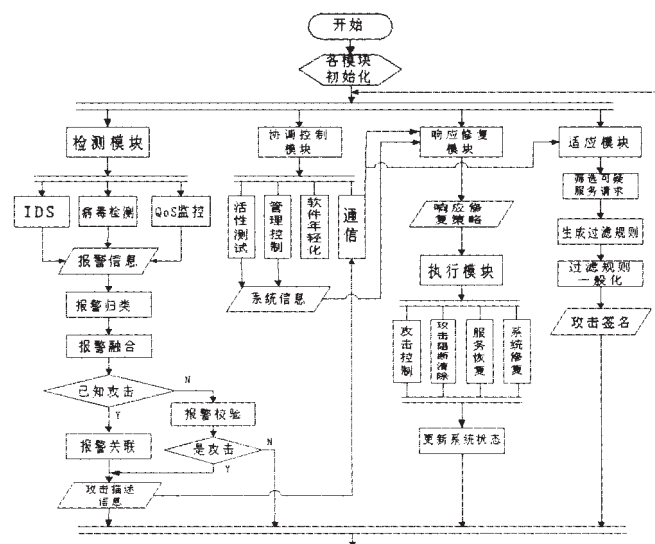


图2 SuNSIA 详细工作流程

6 SuNSIA 的特性分析

在面对攻击、失效的意外事件时,SuNSIA 通过各个模块之间的交互、协作,实现系统最大的生存能力。

6.1 SuNSIA 具有的优良特性

(1)适应未知攻击能力 适应未知攻击的能力是一个

真正有意义的生存系统必备的特性,SuNSIA 中通过适应模块学习能够识别未知攻击。

(2)容忍一定程度上的误报和漏报 通过报警融合、关联,使得系统可以容忍一定程度上的误报;模拟免疫系统协同刺激的报警校验功能对报警信息进行校验,清除其中的误报,使系统能容忍一定程度的误报。

(3)易扩展性 SuNSIA 的易扩展性体现在两个方面:一方面,分布式控制结构允许其所保护的网路规模具有易扩展性;另一方面,SuNSIA 按照面向对象的方法进行设计,SuNSIA 自身体系结构同样具有易扩展性。

(4)良好的自治能力 SuNSIA 能够自主地响应检测到的各种意外事件,尽可能地减少了管理员的参与。

6.2 目前 SuNSIA 中存在以下问题

(1)SuNSIA 中所用到的很多技术现在都不完善,在实际布置时很大程度上需要依靠冗余来弥补这些不足,大量冗余的使用使得系统实现的费用成为一个主要的障碍。

(2)为了减小对应用服务的影响,SuNSIA 中控制系统的分布性是在中小规模局域网一级上实现的,并未达到完全的分布式控制。

7 结论

根据目前尚无公认、成熟的生存网络系统构建方法,缺

乏有效的网络系统生存能力评估方法的现状,以及自然界生物(如人自身)和生存网络系统之间的相似性,提出了一个基于生物免疫原理的生存网络系统——SuNSIA 的构想。虽然目前实际构建 SuNSIA 还会存在一些问题,但是从第 5 节分析不难看出,将生物免疫原理应用到生存网络系统的构建还是非常有效的,可以解决现在生存网络系统构建中存在的很多问题。

参考文献(References)

- [1] R J Ellison, D A Fischer, R C Linger, et al. Survivable Network Systems: An Emerging Discipline [R]. Technical Report CMU/SEI-97-TR-013, 1997, revised 1999
- [2] Benoit Morel. Immunology and the Survivability of Mission Critical Cyber-Based Systems [A]. In: Information Survivability Workshop[C]. (ISW-2001), Vancouver, 2002
- [3] A Somayaji, S A Hofmeyr, S Forrest. Principles of a Computer Immune System [A]. In: Proceeding of New Security Paradigms Workshop, Langdale, Cumbria[C]. 1997, 9: 75~82
- [4] Steven A Hofmeyr. An Interpretative Introduction to the Immune System [A]. In: Appear in Design Principles for the Immune System and other Distributed Autonomous Systems[M]. Oxford: Oxford University Press, 2000

(责任编辑 李慧政)

·封面文字说明·

国家天文台将启动 8 大天文工程

为实现中国天文学研究的跨越式发展,加快追赶世界先进水平的步伐,国家天文台近期将启动实施 8 大天文工程。这 8 大天文工程分别是:大天区面积多目标光纤光谱天文望远镜(LAMOST)、空间太阳望远镜(SST)、500 m 口径球面射电望远镜(FAST)、“宇宙第一缕曙光”探测项目(21CMA)、青藏高原天文台选址计划、云南高美古 2.4 m 望远镜建设、云南抚仙湖红外太阳塔建设以及中国月球探测计划。这些项目将代表中国乃至世界天文技术的最高水平。

以大天区面积多目标光纤光谱天文望远镜为例,该项目建成后将成为世界上光谱获取率最高的望远镜。它可同时观测 4 000 个天体。借助它,天文学家只需两三年时间就能完成对整个宇宙星体的观测任务,而使用普通望远镜则要花费数千年。LAMOST 还能根据星体的光谱分析其化学组成、速度、移动状态等,天文学家依靠这些资料就能为整个宇宙画出立体的三维地图,更精确地构建宇宙模型。该工程将耗资 2.5 亿元人民币,有望于 2007 年年底完工。

空间太阳望远镜将是我国第一个太空望远镜,直径 1 m 的镜头将使其成为世界上最大的空间太阳望远镜。受大气层的影响,在地面观测天体将大大影响观测精度;将望远镜送入太空后,天文学家就可摆脱大气层的干扰,看得更远、更清楚。我国将争取在下一个太阳活动峰年前,也即 2010 年前将空间太阳望远镜送入太空,以巩固我国在太阳

空间研究领域的国际先进地位。

天文学家目前只能观察到距今 130 亿年的星光,再往前追溯就遇到了障碍,除了宇宙大爆炸时留下的一些辐射信号外,人类观察不到其它任何光信号。因此,宇宙大爆炸这一时间段被称为宇宙的“黑暗时代”。宇宙中第一代天体就形成于“黑暗时代”,探寻这一时段宇宙的奥秘是所有天文学家梦寐以求的事。“宇宙第一缕曙光”探测项目则为中国天文学家揭开这一时段的谜底提供了一个机会。在 2006 年该项目建成后,天文学家就可利用布设在新疆乌拉斯台山谷中的 1 万根天线,收集到“黑暗时代”氢元素的特殊辐射信号,看到宇宙中第一批恒星发出的光芒——宇宙的“第一缕曙光”。

长期以来,除了个别领域,我国的天文学研究在整体上落后于欧美国家,导致这种局面的重要原因就是我国缺乏先进的天文设备。天文学是前沿基础科学,提升中国天文学整体水平是国家科技战略的重要组成,对国家的科技发展具有重大推动作用。国家天文台实施 8 大天文工程将投资数十亿资金,据悉,除青藏高原天文台选址计划时间难以确定外,其它 7 项工程预计将在 2010 年全部完成。

本期封面图片为上述 8 大建设工程之一——大天区面积多目标光纤光谱天文望远镜(LAMOST)项目的效果图,由中国科学院国家天文台供稿。