人工免疫技术在农业信息化建设中的应用

周蕾[1,2]　(1 .新疆五家渠石河子大学商学院商务管理系,新疆五家渠831300 ;2 .西安电子科技大学计算机学院,陕西西安710126)

摘要　分析了web 网站在农业信息化建设中的作用和web 网站中的安全问题,介绍了入侵检测技术和人工免疫理论的基本思想以及人工免疫技术在入侵检测领域中的应用。

关键词　农业信息化; 入侵检测; 人工免疫技术
中图分类号　F302 .4　　文献标识码　A　　文章编号　0517 - 6611(2009)13 - 06291 - 02

Research on Artificial Immune Technology in Building Agricultural Information

ZHOU Lei　(Department of Business Management , Business School of Shihezi University , Wujiaqu , Xinjiang 831300)

Abstract　The role of web site in the building of agricultural information was analyzed in this assay , the basic idea of intrusion detection technology and artificial immune and the application of artificial immune technology in intrusion detection field were introduced .

Key words　Agricultural information ; Intrusion detection ; Artificial immune technology

2007 年《中共中央国务院关于积极发展现代农业扎实推进社会主义新农村建设的若干意见》首次将信息化明确为农业"三化"(水利化、机械化、信息化)的一个重要组成部分加以强调,并把"加快农业信息化建设"单独作为一个条目进行全面部署和安排。中央之所以重视农业信息化问题,是因为信息化是社会主义新农村建设的重要组成部分,是农村经济建设、政治建设、文化建设、社会建设和党的建设的重要保障;是实现农村公共服务与社会管理的决策科学化、管理现代化和服务人性化,构建和谐社会的重要因素。

近年来,我国各级政府成功实施了"三电合一"农业信息服务、"金农"工程、百万农民上网工程等;电子信息产业、电信部门实施了"村村通电话"工程,把网络数据光纤延伸到广大农村的每一个村镇,为农业信息化建设打下良好的基础。这在很大程度上有利于将我国农村农业信息传播方式由原来的主要靠开会、办班、发资料、有线广播和有线电视等落后方式,转变为以计算机网络+ web 网站为主体的快速、高效的农业信息服务方式。如何快速、安全可靠地借助web 网站向农民提供准确、及时的农产品供求信息,为农户营造一个安全的网上交易环境,对于真正实现农业信息化具有重要意义。因此,笔者分析了web 网站的安全隐患,介绍了人工免疫技术的基本思想和该理论在入侵检测中的作用,并给出了其抽象结构模型农业信息化的建设提供理论指导。

1　web 网站的安全隐患分析

1 .1　服务器系统　任何操作系统和Web 服务器都存在这样那样的漏洞,尤其是系统默认设置存在很多潜在的威胁,一些黑客和病毒木马就是利用了这些漏洞来破坏系统。另外,一个服务器上安装过多种服务也会降低系统的安全性。服务器系统的安全漏洞主要通过打补丁和系统安全配置来解决。

1 .2　网络用户　服务器系统上的各种用户是构成服务器安全的一大隐患。比如用户的口令强度过弱导致被破解、特殊用户(如guest)的潜在威胁和用户权限设置不当等。通过分组管理系统用户和审核用户的行为可以有效防止这类威胁。

1 .3　web 脚本程序和数据库系统　Web 网站脚本程序和数据库存在两方面的安全问题,一是解释执行脚本的系统和数据库本身的漏洞,比如ASP 的源代码泄漏和SQL 语句的客户资料认证漏洞等;一是程序设计逻辑上存在漏洞,比如身份认证逻辑不严密、重要文件和数据没有加密等。通过为系统打补丁和优化安全认证程序有效降低这类漏洞的危害。

1 .4　黑客入侵　2003 年,CSI/ FBI 调查所接触的524 个组织中,有56 % 遇到电脑安全事件。因与互联网连接而成为频繁攻击点的组织连续3 年不断增加,遭受拒绝服务攻击(Dos)则从2000 年的27 % 上升到2003 年的42 % 。调查显示,521 个接受调查的组织中96 % 有网站,其中30 % 提供电子商务服务,这些网站在2003 年1 年中就有20 % 未经许可入侵或误用网站。更令人不安的是,有33 % 的组织说他们不知道自己的网站是否受到损害。据统计,全球平均每20 s 就发生1 次网上入侵事件,黑客一旦找到系统的薄弱环节,所有用户均会遭殃。我国公安部公布了2006 年全国信息网络安全调查结果,其中关于网络安全事件的分析结果显示[1] :2005 年5 月至2006 年5 月,有54 % 的被调查单位发生过信息网络安全事件,其中,遭到端口扫描或网络攻击的占36 % 。黑客入侵导致的危害有网页内容被篡改、信息泄露等。

上述安全隐患,前3 项是可以通过及时升级软件或打补丁来解决的。但是对于解决黑客入侵的问题,则是不容易的。

2　人工智能与入侵检测技术

2 .1　入侵行为与入侵检测　入侵行为主要是指对系统资源的非授权使用,可以造成系统数据的丢失和破坏、系统拒绝服务等危害。

入侵检测通过对计算机网络或计算机系统中的若干关键点收集信息并进行分析,从中发现网络或系统中是否有违反安全策略的行为和被攻击的迹象。进行入侵检测的软件与硬件的组合就是入侵检测系统。

2 .2　入侵检测系统的工作原理　一个入侵检测系统分为4 个组件:事件产生器(Eevnt generators) ,事件分析器(Event analyzers) ,响应单元(Response units) 和事件数据库(Event databases) 。结构如图1 。事件产生器的目的是从整个计算环境中获得事件,并向系统的其他部分提供此事件;事件分析器分析得到数据,并产生分析结果;响应单元则是对分析结果采取反应的功能单元,它可以作出切断连接、改变文件属性等强烈反应,也可以只是简单的报警;事件数据库是存放各种中间和最终数据的地方的统称,它可以是复杂的数据库,也

作者简介　周蕾(1978 -) ,女,河南汝南人,在读硕士,讲师,从事网络安全和人工智能的教学与研究。
收稿日期　2009-02-23

可以是简单的文本文件。

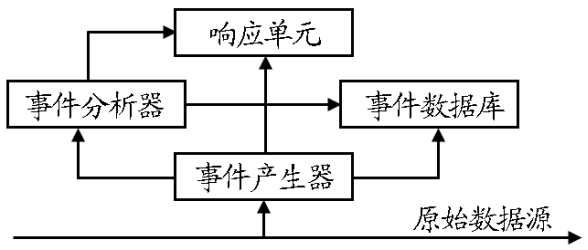

图1 入侵检测系统的组成

Fig.1 The composition of intrusion detection system

入侵检测的第一步是信息收集,收集内容包括系统、网络、数据及用户活动的状态和行为。由放置在不同网段的传感器或不同主机的代理来收集信息,包括系统和网络日志文件、非正常的目录和文件改变、非正常的程序执行以及网络流量。

第二步是信息分析,该模块将收集到的有关系统、网络、数据及用户活动的状态和行为等信息,送给检测引擎,检测引擎驻留在传感器中,一般通过3 种技术手段进行分析:模式匹配、统计分析和完整性分析。当检测到某种误用模式时,产生一个告警并发送给控制台。其中,检测引擎所采用的3 种分析方法基本原理均不同,但是目的都是为了发现入侵行为。

模式匹配就是将收集到的信息与已知的网络入侵和系统已有模式数据库进行比较,从而发现违背安全策略的行为。该过程可以很简单(如通过字符串匹配以寻找一个简单的条目或指令),也可以很复杂(如利用正规的数学表达式来表示安全状态的变化)。该技术已相当成熟,检测准确率和效率都相当高。但是,该方法存在的弱点是需要不断的升级以对付不断出现的黑客攻击手法,不能检测到从未出现过的黑客攻击手段。

统计分析方法首先给系统对象(如用户、文件、目录和设备等)创建一个统计描述,统计正常使用时的一些测量属性(如访问次数、操作失败次数和延时等)。该方法的优点是可检测到未知的入侵和更为复杂的入侵,缺点是误报、漏报率高,且不适应用户正常行为的突然改变。目前常用的统计分析方法如基于专家系统的、基于模型推理的和基于神经网络的分析方法,并正处于研究热点和迅速发展之中。

完整性分析主要关注某个文件或对象是否被更改,这经常包括文件和目录的内容及属性,它在发现被更改的、被特洛伊化的应用程序方面特别有效。完整性分析利用强有力的加密机制(消息摘要函数,如MD5)能识别微小的变化,其优点是不管模式匹配方法和统计分析方法能否发现入侵,只要是成功的攻击导致了文件或其他对象的任何改变,它都能够发现;缺点是一般以批处理方式实现,用于事后分析而不用于实时响应。尽管如此,完整性检测方法还应该是网络安全产品的必要手段之一。

第三步是结果处理,控制台按照告警产生预先定义的响应采取相应措施,可以是重新配置路由器或防火墙、终止进程、切断连接和改变文件属性,也可以只是简单的告警。

2.3 人工免疫技术在入侵检测中的应用 人工免疫技术是将生物体中的免疫机制运用到计算机领域的一种智能技术。自从Farmer 于1986 年提出免疫网络的数学描述以来[2],已经有许多学者致力于将免疫系统理论应用到入侵检测系统的研究[3-7]。免疫理论在入侵检测领域的应用成为近年来的一个新的研究热点[7]。

国内外有些学者对生物体内的免疫机制进行了比较深入的研究[8-9]。生物体内的自然免疫系统是一个结构复杂、功能最为独特的系统。该系统的重要作用就是区分外部有害抗原和自身组织,并产生抗体来清除病原进而保持有机体的稳定。从计算机的角度来看,生物体内的免疫系统是一个高度并行、分布、自适应和自组织的系统,由许多执行免疫功能的器官、组织、细胞和分子等组成,其主要作用是能够辨别“自体”与“非自体”物质,对之做出精确应答,具有很强的学习、识别、记忆和特征提取能力。

人工免疫技术是借鉴自然免疫系统的基本原理和思想,解决计算机应用领域中的一些复杂问题。目前,主要是解决计算机安全系统中发生频繁的、形式变化多样的入侵和攻击的识别或检测问题,然后,可以采取相应的措施进行防御。这种防御能力具有更高的适应性、一般性,通过其自学习、自适应能力来改变传统计算机安全系统中的不断地“发现漏洞— 打补丁”的被动防御方法,实现更一般目标的防御,从而改善计算系统的安全性能。

基于人工免疫技术的入侵检测系统是将整个网络看作是一个被保护的机体,网络中的每一台主机看作是机体中的一个不同的位置。每一台主机都有一个检测器集合,这个检测器集合又分为两个部分:记忆检测器集合和成熟检测器集合,它们分别识别已知的入侵模式和新的入侵模式。一旦一台主机上的成熟检测器识别了一个新的入侵模式,这个检测器就参与本主机的记忆检测器的竞争,同时,将这个检测器作为记忆检测器通过网络传送到其他相关主机参与记忆检测器的竞争,由此,使得一个主机的记忆可以成为整个网络的记忆。最后,检测器根据模式匹配规则对检测到的异常行为进行相应的处理(如报警)。图2 所示为入侵检测系统的抽象模型。

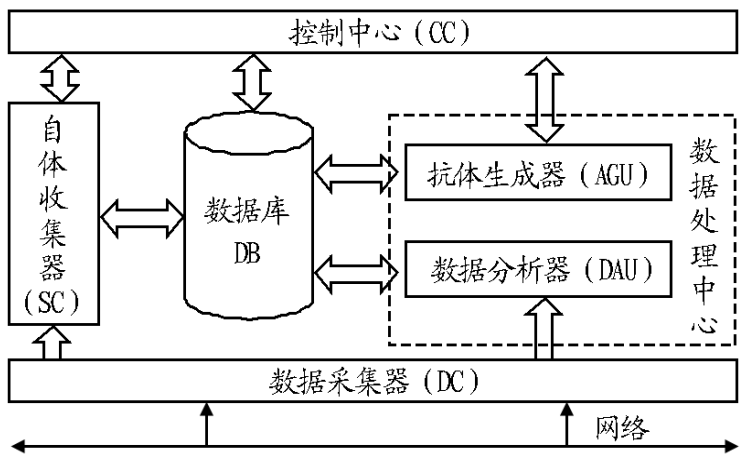

图2 入侵检测系统的抽象模型

Fig.2 Abstract model of intrusion detection system

3 结语

先进的信息技术可以有效地提高web 网站的安全性能,但是还需要有完善的管理制度和监督体制。只有双管齐下才能真正为农业信息化建设提供重要保障。

参考文献

[1] 中华人民共和国公安部.公安部公布2006 年度全国信息网络安全状况暨计算机病毒疫情调查结果[EB/OL].(2006-08-08)http://www.mps.gov.cn/n16/n1237/n1342/130157.htmh.

(下转第6294 页)

3 基于 Matlab 的 RBF 网络函数土壤分类仿真

笔者将RBF-NN 用于土壤分类系统,即用径向基函数神经网络判定土壤分类,也就是用径向基函数神经网络实现从土壤光谱特征向量到类别映射。因此RBF 神经网络的输入土壤光谱特征向量 X 如式(1) 所示。

在 Matlab 软件中,设计 newrbf(P,T,Goal ,Spread) 函数来训练RBF 神经网络,函数中各参数:P 为输入向量,T 为目标输出向量,Goal 为网络均方误差,Spread 为径向基函数伸展常数。其中参数Goal 和Spread 由用户给出。在网络训练的过程中采用 OLS 算法,自适应的增加径向基网络的隐层神经元,来不断减小网络的输出均方差,直至达到Goal 目标时,训练结束。

在实验中,newrbf( ) 函数的2 个重要参数 Goal 和Spread 的取值直接影响到网络训练的时间和网络的拟合,适当的选择上述2 个参数至关重要,通过多次的试算调整组合(Goal , Spread) 取最优值。调整过程中注意保持较大的Spread,保证径向基函数的输入范围足够大,从而使它的输出有较大的值。Spread 越大网络输出越平滑,拟合性越好。

训练样本的选择尽量选择具有代表性、典型的训练样本。笔者选择表1 中典型土壤类型训练样本。实验仿真结果表明(表2) ,Goal 、Spread 值分别取1 000 和100 ,不但分类精度最高,而且所需的训练时间相对较少,说明了并不是训练时间越长得到的分类精度就会越高。如果保持Spread 取值100 不变,减小均方误差 Goal 的值到500 ,可以看到训练时间成倍增加,而分类精度反而下降。这表明如果均方误差设定越小虽然可以提高拟合精度,但网络泛化能力减弱,导致测试精度不高。显然Spread 值取100 是比较合适的,高于或低于这个值都得不到最好的分类精度。

尽管遥感影像本身也反映了因为地形变化导致的土壤光谱反射差异,但它并不能完全代表自然景观中土壤的变异,因此传统分类器的分类总精度在59 % 左右。表2 显示,基于RBF 神经网络的分类精度为68 % 左右,比传统分类器提高了9 % 左右。

表2 神经网络训练情况与分类结果

Table 2 Training situation and mapping results of neural network

神经网络 Neural network	Goal	Spread	训练时间//s Training time	分类精度//% Mapping precision
Net1	1 000	100	695	68 .97
Net2	500	100	3 951	67 .22
Net3	1 000	1 000	1 808	67 .13
Net4	500	500	13 427	61 .48

4 结束语

笔者通过仿真实验验证了径向基函数神经网络在基于遥感图象的土壤分类中的应用价值。仿真结果表明,径向基函数神经网络能够有效地提高分类精度。在仿真过程中需要根据具体的要求对土壤分类函数的2 个重要参数(Goal- 网络均方误差和Spread- 径向基函的伸展常数) 进行认真的选取。RBF 神经网络分类法是基于遥感图象的土壤自动分类系统非常重要的组成部分,该领域的研究对农业、环境、资源可持续利用等方面提供了数据支持。

参考文献

[1] 罗红霞. 基于土壤系统分类的土壤遥感自动识别分类系统的设计[J] . 西南师范大学学报: 自然科学版,2003 ,28(4) :623 - 625 .

[2] 刘焕军, 张柏, 杨立, 等. 土壤光学遥感研究进展J] . 土壤通报,2007 ,38 (6) :1197 - 1199 .

[3] DANIEL K W,TRIPATHI N K,HONDA,et al .Analysis of VNIR(4001100 nm) spectral signatures for estimation of soil organic matterin tropical soils of Thailand[J] .Int J Remote Sensing ,2004 ,25(3) :643 - 652 .

[4] 刘建霞, 王芳, 谢克明, 等. 基于RBF 神经网络的天线阵方向图建模[J] . 太原理工大学学报,2008 ,39(1) :37 - 38 .

[5] 毛永毅, 李明远, 张宝军, 等. 基于RBF 神经网络的AOA 定位算法[J] . 计算机应用,2008 , 28(1) :1 - 3 .

(上接第6292 页)

[2] FARMER J D,PACKARD N H,PERELSON A .The immune system,adaption , and machine Learning[J] .Physica D,1986 ,22 :187 - 204 .

[3] KIM J,PETER J B .Towards an artificial immune system for network intrusion detection: an investigation of dynamic clone selection . Proceeding of world congress on computation intelligence[C] . Piscataway :IEEE Press ,2002 .

[4] DE CASTRO,VON ZUBEN. Artificial immune system: Part I - basic theory and applications[EB/ OL] . ftp :/ / ftp . dca . fee . unicamp . br/ pub/ docs/ vonzuben/ lnunes/ trdca0199 . pdf .

[5] DE CASTRO,VON ZUBEN. Artificial immune system: part II - a survey of applications[EB/ OL] . ftp :/ / ftp . dca . fee . unicamp . br/ pub/ docs/ vonzuben/ lnunes/ trdca0200 . pdf .

[6] HARMER P K, WILLIAMS P D, GUNSCH G H,et al . An artificial immune system architecture for computer security applications[J] .IEEE Transaction on Evolutionary Computation ,2002 ,6(3) :252 - 280 .

[7] JUNG-WON KIM,PETER BENTLEY. The Artificial Immune Model for Network Intrusion Detection[C] .7th European Conference on Intelligent Techniques and Soft Computing(EUFIT'99) ,1999 .

[8] 李涛. 计算机免疫学[M] . 北京: 电子工业出版社,2004 .

[9] 莫宏伟. 人工免疫系统原理和应用[M] . 哈尔滨: 哈尔滨工业大学出版社,2002 .