一种基于人工免疫技术的存储异常检测系统

黄建忠 裴灿浩 谢长生 陈云亮 方允福
(华中科技大学-武汉光电国家实验室-光电信息存储研究部暨华中科技大学-数据存储教育部重点实验室 武汉 430074)

摘 要 绝大部分认证子系统无法保证账户的真实性,它会将冒用盗窃账户的入侵者视为'合法'用户。为了过滤这类非法用户,存储安全子系统必须进行访问行为诊断。为了增强存储预警能力,提出一种基于人工免疫的异常检测方案来监控用户的访问行为。若一个访问请求违反了访问控制规则,它就被视为'异己',从而给存储安全子系统提供一些警告提示。本方案(Storage Anomaly Detection System,SADS)针对存储层的入侵检测,并关注读/写数据请求,同时与网络入侵检测系统协同构筑了两层检测体系。仿真结果显示,SADS能达到相当高的检测率和较低的误警率,验证了方案可行性。而开销测试表明,SADS子模块的时间开销是可接受的(如对3MB的数据,其开销控制在11.6%以内)。

关键词 存储安全性,异常检测,人工免疫系统,用户访问行为
中图法分类号 TP303 **文献标识码** A

Research on an Artificial Immune System-based Storage Anomaly Detection

HUANG Jian-zhong PEI Can-hao XIE Chang-sheng CHEN Yun-liang FANG Yun-fu
(Division of Data Storage System, Wuhan National Laboratory for Optoelectronics, Huazhong University of Science and Technology Key Lab. of Data Storage System, Ministry of Education, Huazhong University of Science and Technology, Wuhan 430074, China)

Abstract Most authentication sub-systems can not guarantee the authenticity of the account, and an intruder using a stolen account may be regarded as a legitimate user. In order to filter out such illegal users, the storage system should be able to watch for the user access activities. In order to enhance the storage security, the paper proposed an immune anomaly detection scheme to identify the anomalous access behavior. When an access request violates the access control rule, it is viewed as Non-self, so as to provide some storage early warning tips to the storage security sub-system. The proposed storage anomaly detection system (SADS) targets the anomaly detection at storage level and focuses on the read/write data requests, constructing two-layer detection together with the network intrusion detection system (NIDS). The simulation results show the proposed scheme can reach rather high detection rate and low false alarm rate, validating its feasibility. The overhead test exhibits that the computation time caused by SADS is acceptable, e. g below 11.6% as to 3MB data.

Keywords Storage security, Anomaly detection, AIS, User access behavior

1 引言

目前,数据已成为企业、机构和个人的最重要资产之一。作为数据存放的平台,存储系统得到越来越多的关注,其包括恶意攻击,如入侵、口令嗅探、木马、蠕虫等。若无必要的存储安全措施,存放数据将成为攻击者的既定目标,因此存储安全逐渐成为研究热点[1]。认证系统在存储安全中扮演重要角色,它包括两个阶段:身份证明和身份验证。尽管身份验证阶段能确保用户身份是有效的,但无法保证身份的真实性。例如,入侵者用一个盗窃账户进行登录,认证子系统将视该入侵者为'合法用户'。为了过滤出这类非法用户,存储安全子系统应该能够进行用户行为诊断。

一些管理标准,比如SNMP,WBEM,WS-MAN,SES,SMI-S等,能用来监控分布式存储系统的状态。这些标准在监测硬件异常时发挥作用,在用户行为诊断上却无能为力。作为人工智能中一种新的计算范例,人工免疫技术(Artificial Immune System,AIS)被应用于许多领域,比如数据挖掘、错误检测、模式识别和异常检测。也就是说,AIS能用于异常检测和计算机安全[2]。

既然AIS具有'自己'/'异己'的分类能力,使用这种生

到稿日期:2009-02-20 返修日期:2009-04-21 本文受国家"973"重大基础研究项目(2004CB318203)和国家自然科学基金(60603074/60603075)资助。

黄建忠(1975—),男,博士,副教授,主要研究方向为网络存储安全和对象存储安全,E-mail:husthjz@126.com;裴灿浩(1971—),男,博士,主要研究方向为磁盘阵列及存储安全性;谢长生(1957—),男,教授,博士生导师,主要研究方向为网络存储系统、采用新原理的超高密度、超高速存储技术等。

物隐喻处理相似问题，如识别异常用户行为就变得有意义。行为/行动若违背了访问控制规则，将被视为‘异己’，那么就有可能将‘异己’行为和‘自己’行为识别出来，从而给存储安全子系统提供一些警示信息。出于实时性和自适应性考虑，本文基于 AIS 提出一种新的异常检测方案即存储异常检测系统(Storage Anomaly Detection System，SADS)来监测异常的存储访问行为。

2 相关技术

2.1 异常检测问题

在不同的应用场合，异常检测具有不同的含义。通常，异常检测问题可视为一个分类问题，即从给定的问题空间中给定一个元素，系统应该能将之区分为正常或异常。换句话说，异常检测等同于判定未知数据是否由正常的数据源生成。另外，异常检测问题与变化检测、异常过滤或分类问题相似。在存储系统中，入侵将导致存储数据的改变，因此将存储层的入侵检测称为存储异常检测。目前，已有几种技术比如基于规则的过滤、统计方法、隐性马尔可夫模型技术、数据挖掘技术等，用于解决异常检测问题，这些技术多用于网络入侵检测(Network-based Intrusion Detection System，NIDS)，甚少用于存储异常检测。

从实现角度看，NIDS 是在特定的网络接口上执行入侵检测的，它往往嵌入到防火墙中，扫描网络流量并监测可疑的攻击信号。相较于 NIDS 针对网络流量，基于存储的入侵检测系统(Storage-based IDS，SIDS)针对底层的读/写数据请求[3]，同时检测模块和存储数据之间具有更短的数据通道，从而能直接监控数据的变化。作为一种特定的 SIDS，本文提出的 SADS 将关注存储元数据的异常检测。

2.2 已有异常检测方案

现有的几种异常检测方案中，基于规则或信号的检测方案是最普遍的。它采用攻击‘信号’来识别潜在的攻击，然后对可疑的网络流量进行警告[4]。基于统计的检测系统则不同，它先指定‘正常’网络活动，所以落在‘正常’范围外的流量都被标记为‘异常’[5]。基于轮廓(Profile)的异常检测中，检测系统用几种数据分析技术为网络主机创建一个轮廓，然后使用这些轮廓进行异常检测，轮廓能降低代表用户行为向量的维度[6]。基于规范的异常检测采用手工制定的规范来描述合法的系统行为，该规范能简洁地表达异常信息特征[7]。基于隐形马尔可夫模型(HMM)的异常检测则采用隐形马尔可夫模型从‘正常’训练数据中建立‘正常’轮廓，再用这些轮廓去辨别异常活动[8]。

上述各种异常检测方法均在某特定应用中表现良好，但各自存在不足之处。比如，基于规则检测系统在检测新的攻击时效率很低；基于规范异常检测能达到很低的误警率，但制定规范是相当耗时的；基于 HMM 异常检测的检测速度很高，但建立相应的马尔可夫模型需要很长时间。

2.3 人工免疫系统

人体通过多层免疫系统保护自身免遭外来入侵者侵蚀，该多层免疫系统由物理屏障、生理屏障和免疫系统组成。免疫系统包括大量不同的代理，它们相互合作来检测抗原。在免疫系统中存在两类淋巴细胞，称为 T 细胞和 B 细胞。T 细胞是免疫防御的主要驱动力，而 B 细胞负责抗体的产生和分泌。两种细胞都在骨髓中产生，并最终在身体血液和淋巴血管中循环[9]。免疫交互过程如图 1 所示。

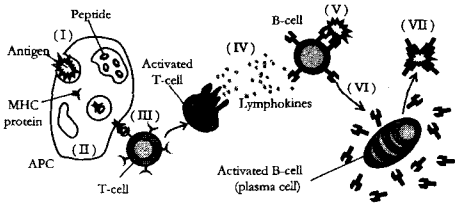

图 1 免疫系统中的交互过程

免疫系统是高度进化的生物系统，能识别病原体，因此一些研究者借鉴其信息处理能力来解决工程问题，特别是用于计算机安全。例如，Forrest 教授的研究组将 AIS 应用于入侵检测[10]；Kim 博士研究基于 AIS 的网络入侵检测[11]；Terri Oda 采用 AIS 设计了一个垃圾邮件检测系统[12]等。

2.4 基于 AIS 的异常检测

辨别‘自己’和‘异己’是生物免疫系统的一个主要机制，而阴性选择则是过滤出胸腺中自反应淋巴细胞的一个过程。受阴性选择规律的启发，Forrest 教授提出了一种阴性选择算法(Negative Selection Algorithm，NSA)。NSA 的基本思想是在补充空间生成一组检测器，并使用这些检测器对未知数据进行分类，用于异常的检测[10]。通常，NSA 包括以下几个步骤：1)在空间 U 将‘自己’定义成长度为 L 的一组元素 S；2)生成一组检测器 D，使得每个检测器无法与 S 中任一元素匹配；3)连续将 D 中检测器与 S 匹配，以监控 S 的变化。这里‘自己’集和‘异己’集构成了空间 U，即 $U=S\cup N$ 且 $S\cap N=\varnothing$。

从 NSA 的描述看，其检测器生成算法随检测生成过程、匹配规则和呈现方案的不同而不同，因此随后出现了许多阴性选择算法的变种。例如，线性 NSA 和贪婪 NSA 依据生成/淘汰机制而提出；r-chunks 方案、海明距离、欧几里德距离依据匹配规则而提出；二进制/字符串呈现、实数呈现从数据表示的角度提出；超球体、超立方体和混合表示方式则从检测器呈现方式的角度提出。

为改进异常检测，Gonzalez 博士为阴性选择算法研究了不同的检测器呈现方案，包括超长方体、模糊规则和超球体，并提出了 4 种不同的检测器生成算法：实数阴性选择算法(RNS)、融合检测规则的阴性选择算法(NSDR)、随机实数阴性选择算法(RRNS)、模糊规则的阴性选择算法(NSFDR)[13]。

3 存储异常检测系统

3.1 元数据的免疫模型

在大规模存储系统中，很难检测所有数据的异常，因为数据量通常是巨大的。既然元数据是描述其它数据的数据，即关于数据的数据，我们能通过监控元数据来发现数据的变化。这种方法能降低检测系统的计算和设计复杂度。这里参考了一般的存储免疫模型[14]，并为存储元数据的变化提出了一种简化的免疫模型，如图 2 所示。

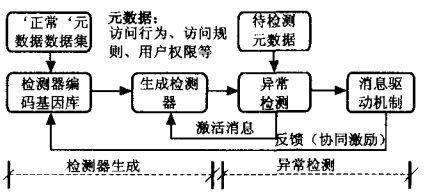

图 2 存储元数据的免疫模型

上述存储免疫模型模仿了生物免疫模型，它和阴性选择

过程是一致的，所有的免疫模块协同工作来完成异常检测。该免疫模型描述了免疫过程的两个主要阶段：检测器生成阶段和异常检测阶段。修改、嗅探和破坏存储元数据的行为或现象称之为异常，它包括数据的非完整性、恶意脚本、特洛伊木马、蠕虫、病毒和未授权访问等，而存储元数据则指访问规则、文件属性、用户权限等。

3.2 两层检测的体系结构

将 NIDS 置于存储网络的边界，并将 SADS 嵌入到每个存储节点的文件系统中，便能构建一个两层的入侵/异常检测结构，如图 3 所示。存储异常检测模块作为堆叠式文件系统单元装载到文件系统中，堆叠式文件系统是一种按增量方式往现有文件系统添加功能、特性的有用技术[15]，并作为内核模块进行加载；它装载在底层物理文件系统之上，截获并操纵流经文件系统的事件和数据。

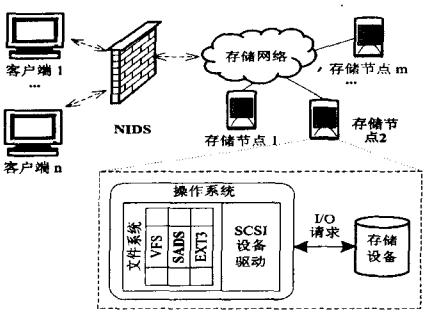

图 3 两层检测的原理图

3.3 SADS 总的工作流程

如图 4 所示，存储异常检测系统 SADS 的工作流程如下：1)收集一批事先判别是合法的行为信息，并采用某种阴性选择算法建立起异常行为抗体基因库；2)当系统正常运行时，截获访问序列，并按图 5 所示的存储元数据格式进行变换，构造出对应的抗原序列；3)系统对新进抗原序列(对应存储访问行为)进行匹配，根据匹配结果赋予一定的数值，并更新匹配抗体的权值；4)周期性地对抗体库进行更新，淘汰无用抗体，生成新的有用抗体。通过上述更新过程，存储异常检测系统能够识别出合法的访问行为和不断变化的异常行为。

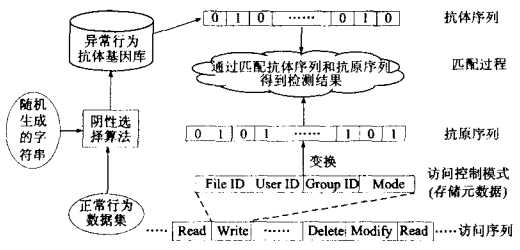

图 4 存储异常检测的工作流程

3.4 存储元数据及其变换

网络存储系统通常采用优化的 Linux 操作系统将物理存储设备挂载到网络上，给客户端提供存储服务。来自客户端的访问请求将发起一个或多个进程，这些进程将进一步调用低层的系统调用。在网络存储系统中存在几百个系统调用，但与文件访问相关的系统调用的数量是相当小的，因此本存储异常检测系统只关注特定的系统调用，比如'open'，'fstat'，'mmap'，'read'，'uname'，'write'，'create'，'close'等。通过监控这些系统调用，日志收集器能截获相关的访问信息，包括用户标识符、文件标识符、组标识符、访问模式。提取的访问信息将被分解成访问序列，而该访问序列将被转换成抗原序列，充当存储行为。

假设每个文件或文件夹的访问控制模式(即存储元数据)的格式如图 5 所示，它表明 FileID 文件允许属于 GroupID 组的用户 UserID 拥有特定的访问权限。所有文件或文件夹的访问控制模式按特定的格式转换成训练数据集(即异常行为抗体基因库)。当一个用户访问一个文件或文件夹时，文件系统将获得这类访问信息(如用户名、组标识、访问模式)。这些访问信息也按图 5 所示的格式进行组织，然后这些信息将被转换成连续数据格式，充当测试数据(即抗原序列)。最后，可使用 AIS 中的技术或算法进行异常检测操作。

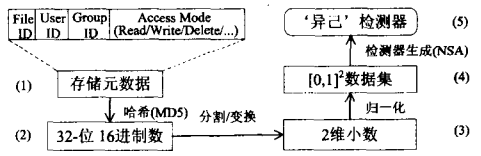

图 5 从存储元数据生成'异己'检测器的过程

RNS 算法针对的是连续数据，在一个超立方体空间上操作，每个检测都有一个中心和一个'异己'识别半径，而检测器之间的距离则通过欧几里德距离公式进行计算。每个系统调用将映射到一个自然数上，如 open→0，fstat→1，read→2，write→3，等等。我们能提取现有'合法'的存储元数据并按图 5 所示的过程获得'自己'训练数据集，再采用 NSA 算法生成'异己'检测器。

3.5 算法适用性考虑

在 NSA 算法中，匹配规则应该精确地描述问题空间中的数据相似性。r-chunk 是一种在字符串呈现空间中使用的匹配规则[16]。这里，如果 r-chunk 检测器 d 的所有字位与字符串 x 中 r 个字位在窗口 w 中全部匹配，则称检测器 d 与字符串 x 匹配。字符串呈现方式有其局限性，包括理解性问题、潜在的扩展性问题、难以与其它技术合并的问题，因此对 NSA 而言，采用实数呈现方式是必要的。本研究中 SADS 采用了 V-detector 算法，它是 RNS 中的最新模型，其采用的基于欧几里德距离的匹配规则对所有维度都进行了同等考虑[17,18]。

首先，根据用户访问权限和访问规则在基因库中构造一组异常规则的预定义集合。为了捕捉访问活动，日志收集器被当作一个模块插入文件系统。SADS 使用实数 NSA 来识别异常访问，这里有效的检测器是无法与存储系统中出现的正常访问相匹配的。为了降低误警率，这里采用了激活阈值，只有当每个检测器达到特定的匹配次数，它才有可能被激活。管理员对报警信息的判断将充当协同激励的一个激活信号，如图 2 中所示的反馈过程。

4 仿真测试

4.1 数据集的准备

试验需要'自己'训练测试数据集和测试数据集。通常，训练数据集来自实际的访问规则、访问权限、访问模式等元数据信息，如访问控制列表文件。按图 5 的步骤，首先能得到一组 32 字位的 16 进制数据，然后将该 16 进制数据划分并归一化成二维数据集，以充当训练'自己'数据集。这里，每个二维数据代表一个点的坐标。

对于训练数据集，采用合成的方式加以生成，方法如下：将训练'自己'数据的一部分子集作为'正常'数据，合成一些

不属于训练'自己'数据的身份数据作为'异常'数据。采用和训练数据集相同的生成过程，便能将测试数据转换成二维数据集。合成方法能简化试验测试过程，因为可通过比较检测结果和测试数据集获得直接明了的统计结果。这里，构造了一个1000数据样本的测试数据集，其中包括950个异常样本。

4.2 实数阴性选择算法的验证

实验中采用了V-Detector这一实数NSA算法，在该算法中，有两个参数会影响检测效果，即'自己'半径和目标覆盖率。如果一个元素距离一个'自己'样本足够近，这种靠近程度被指定为'自己'半径(Self Radius)；而被检测器集所覆盖的'异己'空间的比例称之为'检测器覆盖率'(Coverage)。检测率和误警率是描述检测效果的两个关键因素，在一个基于AIS的分类系统中，检测率通常指检测器检测出的'异己'样本占总异常样本的比例。

采用4.1节所描述的方法，能构建出一组训练数据集，并合成一组测试数据集。'自己'半径为0.06，'检测器覆盖率'为0.99，在4种不同环境下进行了仿真，可以看到采用V-Detector这种实数阴性选择算法(即表1中'边界感知'为'是'，且'检测器大小'为'可变'的情况)具有较好的检测率，检测率为938/950≈98.7%。

表1 在不同条件下检测到的异常数目

检测到的异常数量（总共950个异常）		是否边界感知	
		是	否
检测器大小是否固定	是	879	663
	否	938	746

4.3 仿真测试

上面提到，检测率通常指检测器检测出的'异己'样本占总异常样本的比例。若给定真阳性(True Positive，TP)、假阳性(False Positive，FP)、真阴性(True Negative，TN)和假阴性(False Negative，FN)，则检测率等于TP/(TP+FN)，而误警率则计算成FP/(FP+TN)。同样，在V-Detector算法中，参数'自己'半径和'目标覆盖率'能影响检测效果。这里用仿真方式展现这两个参数分别对检测器数量、检测率和误警率的影响。

采用与4.2节相似的方法，能得到一组训练数据集和一组测试数据集。采用V-Detector算法，得到一组仿真结果，分别如图6、图7和图8所示。其中，'自己'半径从0.01变化到0.10，间隔为0.01；而目标覆盖率分别为0.90和0.99。

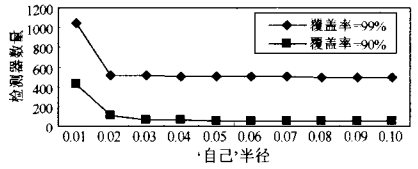

图6 平均检测器数目的变化曲线

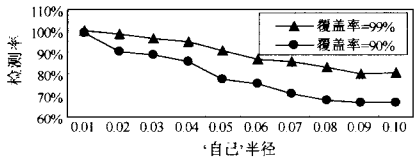

图7 平均检测率的变化曲线

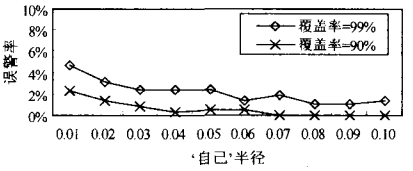

图8 平均误警率的变化曲线

4.4 销测试

为了实现SADS，使用了FiST生成的堆叠式文件系统模板作为基础，并增加了大约5000行C语言代码。对于SADS引起的性能开销，将SADS系统模块堆叠到常用的EXT3文件系统之上，并和EXT3文件进行比较，即Ext3 vs. Ext3+SADS。实验时的硬件环境如下：Intel Core 2 Duo CPU (E6300@1.86GHz)，1GB内存和80GB IDE希捷硬盘(ST380812A)；软件环境如下：操作系统是红帽子Linux 9.0，内核版本是2.4.20-8。实验开发了一个测试程序，以在一组不同文件上间断地执行'读'操作，并记录耗用的访问时间。在进行每一组实验时都进行先卸载、后装载的过程，以避免热缓存效应(Hot Cache)。在Ext3和Ext3+SADS环境下，对文件file0—file9分别运行该测试程序。上述文件大小是不同的，测试结果如表2所列。

表2 Ext3和Ext3+SADS的读操作时间

文件名	File0	File1	File2	File3	File4	File5	File6	File7	File8	File9
文件大小(MB)	1.56	3.03	4.93	16.1	33.6	59.2	98.1	224.3	369.1	624.8
Ext3(sec)	0.1317	0.2523	0.4187	1.3591	2.7820	4.8872	8.0941	18.4702	30.533	51.098
Ext3+SADS(sec)	0.1599	0.2816	0.4490	1.3882	2.8114	4.9170	8.1228	18.5003	30.561	51.128
开销(sec)	0.0282	0.0293	0.0303	0.0291	0.0294	0.0298	0.0287	0.0301	0.0280	0.0301
百分比	21.4%	11.6%	7.23%	2.14%	1.05%	0.61%	0.35%	0.16%	0.09%	0.06%

为了完成对比测试，即只关注读操作的性能影响，允许SADS忽略检测结果。另外，事先进行检测器生成过程，因此SADS的开销主要包括抗原序列生成、抗原-抗体匹配和间接的堆叠层调用。也就是说，表2中列出的SADS开销不包括抗体序列的训练时间。

4.5 分析

从表1和图6可得到如下判断：V-Detector算法能用更少的检测器(即500个检测器)覆盖更多的'异己'空间(即938个异常)。也就是说，V-Detector使用更少的检测器就能获得更好的结果。

仿真结果表明：1)'自己'半径越小，将导致越高的检测率，如图7所示；2)所提出的存储异常检测系统能达到一个相当高的检测率，如'自己'半径为0.05，目标覆盖率为99%时，检测率大约为90%；3)误警率通常低于4%，如图8所示。

SADS的实验结果表明不同文件的读访问时间几乎相同。从时间开销的角度看，本研究提出的通过检测存储元数据的检测方案效果良好。例如，对于不断访问的文件(如大小为3MB的文件)，SADS的时间开销增加了大约11.6%，这种开销是可以接受的；另外，抗体基因库可以在异常检测的前期进行构建，并在检测阶段进行更新。

结束语 出于两个原因，AIS在异常检测中的应用是一个有吸引力的想法：1)生物免疫提供一个高层次的保护，抵御

抗原；2）当前的安全技术无法处理日益复杂的计算机威胁。人们希望从生物获取灵感的方法，如 AIS，以满足这些挑战。

本研究针对存储元数据，提出一种新颖的免疫存储异常检测方案来监控存储访问行为。经过分析和类比，AIS 模型能成功地适用于存储异常检测，其检测系统能识别合法的访问行为和各种异常行为。仿真结果揭示，本方案能达到较高的检测率和较低的误警率。开销测试表明 SADS 造成的性能损耗是可接受的。因此，存储异常检测将有助于增强存储系统的预警能力并提高存储系统的安全性。

参 考 文 献

[1] 舒继武. 网络存储安全[J]. 中国教育网络，2007(11)

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

[3] Pennington A G, Strunk J D, Griffin J L, et al. Storage-based Intrusion Detection: Watching storage activity for suspicious behavior[C]// Proceedings of the 12th USENIX Security Symposium. 2003:137-151

[4] Gopal R K, Meher S K. A Rule-based Approach for Anomaly Detection in Subscriber Usage Patter[J]. Int. J. of Mathematical, Physical and Engineering Sciences, 2007, 1(3):171-174

[5] Qayyum A, Islam M H, Jamil M. Taxonomy of Statistical-based Anomaly Detection Techniques for Intrusion Detection[C]// Proceedings of the IEEE Conference on Emerging Technologies (ICET'05). 2005:270-276

[6] Durgin N A, Zhang P C. Profile-based Adaptive Anomaly Detection for Network Security[R]. SAND2005-7293. 2005

[7] Sekar R, Gupta A, et al. Specification-based anomaly detection: a new approach for detecting network intrusions[C]// 9th ACM Conference on Computer and Comm. Security. 2002:265-274

[8] Du Y, Wang H Q, Pang Y G. A Hidden Markov models-based Anomaly Intrusion Detection Method[C]// Proceeding of WICA'04. 2004:4348-4351

[9] De Castro L N, Von Zuben F J. Artificial Immune Systems: Part I-Basic Theory and Applications[R]. RT DCA 01/99. 1999:1-95

[10] Forrest S, Perelson A S, Allen L, et al. Self-nonself Discrimination in a Computer[C]// Proceedings of the 1994 IEEE Symposium on Security and Privacy. Los Alamitos, CA, 1994:202-212

[11] Kim J, Bentley P J. Towards an Artificial Immune System for Network Intrusion Detection: An Investigation of Dynamic Clonal Selection[C]// Proceeding of Congress on Evolutionary Computation. 2002:1015-1020

[12] Oda T, White T. Immunity from spam: An analysis of an Artificial Immune System for Junk Email Detection[C]// Proceeding of the 4th International Conference on Artificial Immune Systems (ICARIS'05). 2005:276-289

[13] Gonzalez F A. A study of artificial immune systems applied to anomaly detection[D]. the University of Memphis, 2003

[14] Huang J Z, Xie C S, Zhang C F, et al. Security Framework for Networked Storage System based on Artificial Immune System [C]// Proceeding of 5th MIPPR. Proc. SPIE. Vol. 6790, 2007

[15] Zadok E, Nieh J. FiST: A Language for Stackable File Systems [C]// Proceedings of the Annual USENIX Technical Conference. San Diego, CA, June 2000:55-70

[16] Balthrop J, Esponda F, Forrrest S, et al. Coverage and Generalization in an Artificial Immune System[C]// Proceedings of the Genetic and Evolutionary Computation Conference (GECCO'02). 2002:3-10

[17] Ji Z, Dasgupta D. Augmented negative selection algorithm with variable-coverage detectors[C]// Proceedings of 2004 Congress on Evolutionary Computation (CEC'04). 2004:1081-1088

[18] Ji Z, Dasgupta D. Applicability Issues of the Real-valued Negative Selection Algorithms[C]// Proceeding of Genetic and Evolutionary Computation Conference (GECCO'06). ACM Press, 2006:111-118

(上接第 27 页)

[22] Bello L L, Mirabella O, Raucea A. Design and Implementation of an Educational Testbed for Experiencing with Industrial Communication Networks[J]. IEEE Transactions on Industrial Electronics, 2007, 54(6):3122-3133

[23] Krommenacker N, Lecuire V. Building Industrial Communication Systems Based on IEEE 802.11g wireless technology[C]// IEEE Conference on Emerging Technologies and Factory Automation. 2005:71-78

[24] Haertig H, Loeser J. Using switched Ethernet for hard real-time communication[C]// International Conference on Parallel Computing in Electrical Engineering. 2004:349-353

[25] IEC 2004b. IEC65C/341/NP. Real - time Ethernet : Modbus - RTPS[S]. 2004

[26] IEC 2004c. IEC65C/361/NP. Real - time Ethernet: EtherNet / IP with time synchronization[S]. 2004

[27] Pantoni R P, Brandão D. Developing and implementing an open and non-proprietary device description for foundation fieldbus based on software standards[J]. Computer Standards & Interfaces, 2009, 31:504-514

[28] IEC 2004a. IEC65C/359/NP. Real - time Ethernet : ProfiNet IO [S]. 2004

[29] IEC 2004h. IEC65C/353/NP. Real - time Ethernet : TCnet [S]. 2004

[30] IEC 2004i. IEC65C/352/NP. Real-time Ethernet: Vnet/IP[S]. 2004

[31] IEC 2004g. IEC65C/355/NP. Real-time Ethernet: Ethercat[S]. 2004

[32] IEC 2004f. IEC65C/356/NP. Real - time Ethernet : Powerlink [S]. 2004

[33] IEC 2004e. IEC65C/358/NP. Real-time Ethernet: Sercos III[S]. 2004

[34] Miorandi D, Pitturi S. Hybridwired/wireless implementations of Profibus DP: A feasibility study based on Ethernet and Bluetooth[J]. Computer Communications, 2008, 27(10):946-960