ISSN 1009-3044
Computer Knowledge and Technology 电脑知识与技术
Vol.5,No.22, August 2009, pp.6119-6121

E-mail: info@cccc.net.cn
http://www.dnzs.net.cn
Tel:+86-551-5690963 5690964

基于 snort 与免疫原理混合入侵检测系统模型设计

吕秀华

(东南大学 软件学院,江苏 南京 210096)

摘要:该文对 snort 入侵检测系统及基于免疫原理的入侵检测技术进行了探讨和研究,利用 snort 系统作为误用检测系统,把人工免疫的算法应用到异常检测,用于检测未知攻击。在此基础上设计了混合模式入侵检测系统。

关键词:入侵检测;免疫原理;误用检测;异常检测

中图分类号:TP311 **文献标识码**:A **文章编号**:1009-3044(2009)22-6119-03

Based on the Principle of a Mixed Immune Snort and Intrusion Detection System Model Design

LV Xiu-hua

(Software Institute of Southeast University, Nanjing 210096, China)

Abstract: In this paper, exploring and studying the snort Intrusion Detection System and Immune Principle of intrusion detection technologies.Using of snort system as misuse detection system and the artificial immune algorithm is applied to anomaly detection, for detecting unknown attacks. On this basis the design of a mixed-mode Intrusion Detection System.

Key words: intrusion detection; immune principle; misuse detection; anomaly detection

随着信息技术的发展,计算机成为社会活动中的必不可少的工具,大量重要的信息存储在系统中,同时,连入网络中的计算机数量也在成倍增加,这些都使得信息安全问题日益严重。网络安全是网络及应用领域中一直研究的关键问题,常见的网络安全技术主要有身份验证、访问控制、加密技术、数字签名技术、防火墙技术与入侵检测技术。入侵检测技术是防火墙技术的有利补充,是一种对网络传输进行实时监视,在发现可以传输时发出报警或者采取主动反应措施的网络安全技术。入侵检测已经成为网络安全的一个重要的研究领域。

本文对 snort 入侵检测系统及基于免疫原理的入侵检测技术进行了探讨和研究,利用 snort 系统为误用检测系统,把人工免疫的算法应用到异常检测,用于检测未知攻击。在此基础上设计了混合模式入侵检测系统。

1 入侵检测技术介绍

入侵检测技术主要有两种:误用检测和异常检测。

误用检测(Misuse Detection)是假定所有入侵行为和手段(及其变种)都能够表达为一种模式或特征,那么所有已知的入侵方法都可以用匹配的方法发现。误用检测的关键是如何表达入侵的模式,把真正的入侵和正常行为区分开来。误用检测的优点是可以有针对性地建立高效的入侵检测系统,其主要缺陷是不能检测未知的入侵,也不能检测已知入侵的变种,因此可能发生漏报。

异常检测(Anomaly Detection)是假定所有入侵行为都是与正常行为不同的。异常检测需要建立目标系统及其用户的正常活动模型,然后基于这个模型对系统和用户的实际活动进行审计,以判定用户的行为是否对系统构成威胁。常用的异常检测方法有:专家系统、神经网络、机器学习、和人工免疫等。异常检测的关键问题是:① 特征量的选择。异常检测首先是要建立系统或用户的"正常"行为特征轮廓,这就要求在建立正常模型时,选取的特征量既要能准确地体现系统或用户的行为特征,又能使模型最优化,即以最少的特征量就能涵盖系统或用户的行为特征。 ②参考阈值的选定。因为在实际的网络环境下,入侵行为和异常行为往往不是一对一的等价关系,这样的情况是经常会有的:某一行为是异常行为,而它并不是入侵行为。同样存在某一行为是入侵行为,而它却并不是异常行为的情况。这样就会导致检测结果的虚警和漏警的产生。由于异常检测是先建立正常的特征轮廓作为比较的参考基准,这个参考基准即参考阈值的选定是非常关键的,阈值定的过大,那漏警率会很高;阈值定的过小,则虚警率就会提高。合适的参考阈值的选定是影响这一检测方法准确率的至关重要的因素。

误用检测能够较好地检测已知类型的攻击,通常误报率较低,因此大多数的商业 IDS 都采用这种方式。但是,该类型的系统无法检测未知类型的攻击。面对层出不穷的新型攻击显得捉襟见肘。异常检测虽然可以检测未知类型的攻击,但又伴随着较高的误报率,而且检测算法的复杂度一般较高,所以在实际环境中的应用不是很广。由于异常检测和误用检测这两种方法各有所长,选择其中一种方法忽视掉的入侵很可能会被另外一种所识别。因此,可以通过寻找一种有效的协调方式把误用检测和异常检测结合起来,发挥两者各自的优点。弥补各自的缺点,从而获得更好的性能。

2 snort 系统分析

Snort 是目前使用最广泛的开放源代码入侵检测系统, 它具有实时数据流量分析和对网络上的 IP 网络数据包日志进行测试等功能,能够进行协议分析,完成内容搜索/匹配。它能够检测各种不同的攻击方式,对攻击进行实时报警。此外,Snort 具有很好的扩展性和可移植性。从本质上来说,Snort 是一个基于误用检测的 IDS。snort 系统是通过一个已有的规则库进行人侵行为的检测,其中没有规则的扩充机制,这就使得它对于新的攻击行为无能为力。

2.1 snort 系统架构

Snort 入侵检测系统主要由四部分组成:数据包嗅探器、预处理器、检测引擎、报警输出模块。系统体系结构如图 1 所示。

收稿日期:2009-06-02

2.2 snort 系统工作流程

Snort 的基本功能是数据包嗅探器，数据包嗅探是 Snort 工作的开始，Snort 取得数据包后先用预处理插件处理，然后经过检测引擎中的所有规则链，如果检测到有符合规则链的数据包，则系统就会根据输出设置把该信息记录到文件并报警。Snort 的预处理器、检测引擎和报警模块都是插件结构，插件程序按照 Snort 提供的插件接口完成，使用时动态加载，在不用修改核心代码的前提下使 Snort 的功能和复杂性扩展更容易。既保障了插件程序和 snort 核心代码的紧密相关性，又保障了核心代码的良好扩展性。

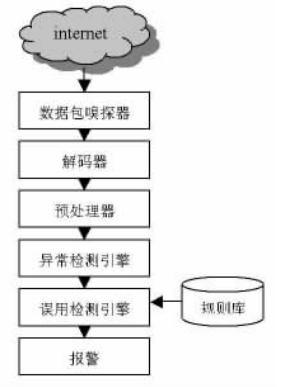

图 1

3 人工免疫原理与入侵检测

3.1 生物免疫系统

生物免疫系统(Biology Immune System，BIS)是一个分布式、自组织和具有动态平衡能力的自适应复杂系统。它对外界入侵的抗原(Antigen，Ag)，可由分布全身的不同种类的淋巴细胞产生相应的抗体(Antibody，Ab)，其目标是尽可能保证整个生物系统的基本生理功能得到正常运转。生物免疫系统具有良好的多样性、耐受性、免疫记忆、分布式并行处理、自组织、自学习、自适应等特点，这些诱人特性，引起研究人员的普遍关注。

人工免疫系统(Artificial Immune System，AIS)就是研究、借鉴、利用生物免疫系统的原理、机制而发展起来的各种信息处理技术、计算技术及其在工程和科学中的应用而产生的多种智能系统的统称。计算机免疫系统是人工免疫、计算机科学的一个分支，是继神经网络、模糊系统、进化计算、人工免疫等研究之后的又一个研究热点。在众多的研究领域中，引入免疫概念后取得了满意的成果，特别在计算机病毒防治、网络入侵检测上，基于免疫的网络安全技术克服了传统网络入侵检测系统的缺陷，被认为是一条非常重要且有巨大实际应用前景的研究方向。

3.2 免疫算法

Forrest 等研究人员受生物免疫系统启发提出了否定选择算法。否定选择，又称阴性选择。否定选择的主要思想是：建立一个随机检测器集，从中进行选择，将对系统无害的自体信息排除，剩下的则认为是异常体的集合。

本文提出的检测器生成器算法(如图 2)是在原有的否定算法的基础上进行了改进。利用误用检测模式先检测出已经确定的攻击模式，对于未知的异常数据则用免疫算法的检测器检测，因此本文的检测器生成是以少量的异常数据为基础生成的，而不是一种不可能存在的模式，这样，产生的检测器数量不会像原始算法产生的那么多，这些检测器是有效的，有利于提高检测效率，节约存储空间。

4 系统设计

4.1 系统设计思路

Snort 基于误用检测技术，其检测能力受到规则数据库中规则的限制，无法检测到未知类型的入侵行为，而基于免疫的异常检测技术的优点是能够检测到未知类型的入侵行为。

一般情况下，网络中绝大部分数据包都是正常的，可以在 Snort 检测引擎之前加入异常检测引擎来过滤掉大部分正常数据。减少 Snort 检测引擎的负担，提高其检测效率；由于 Snort 支持插件方式，因此将异常检测引擎编写成插件，通过 Snort 提供的插件接口，使用时动态加载，可方便地实现在 Snort 中添加异常检测的功能。对于那些不符合网络正常行为模型的数据包，可将其视为异常数据包，先送至误用检测引擎作进一步的检测。经过误用检测引擎未发现入侵行为的异常数据包很可能是新的入侵行为产生的数据包，对这些异常数据包再通过免疫的异常检测模块可以判断是否新的入侵行为模式，然后将这些入侵行为模式转换为 Snort 入侵检测规则并添加到规则库中，这样误用检测引擎就可以检测到新的入侵行为。

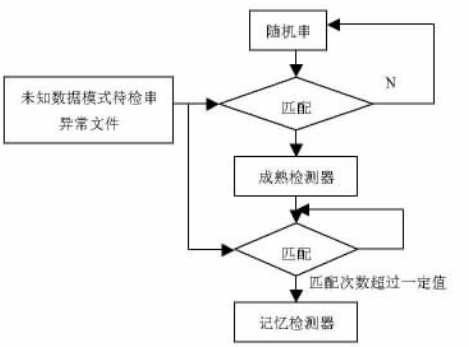

图 2　基于免疫机制的检测模型

4.2 系统架构

本文提出的检测模型系统架构如图 3 所示。

系统主要包括 6 个功能模块：

数据包捕获和解码子系统，用来捕获网络的传输数据并按照 TCP/IP 协议的不同层次将数据包进行解析；

数据预处理，是介于解码器与检测引擎之间的可插入模块，提供一些对解码后的数据包及一些应用层协议的附加处理及解码功能；

异常检测引擎，负责对数据包进行检测，并过滤掉正常的数据包；并将可疑的异常数据包输出到 snort 误用检索引擎模块；

Snort 误用检测引擎模块，把获得的网络数据与规则库进行比较，如果匹配，则报警；否则，作为异常数据存入异常文件；

基于免疫原理检测模块，对异常文件数据进行免疫检测，检测出新的入侵行为模式，调用报警模块，并转换为符合 snort 规则语法的入侵检测规则，然后添加到规则库中。

该系统的主要优点：结合了误用检测与异常检测的优点，提高了检测效率，应用免疫原理提高了检测未知攻击的检测的能力，可以不断更新规则库，检测某些新变种的入侵。

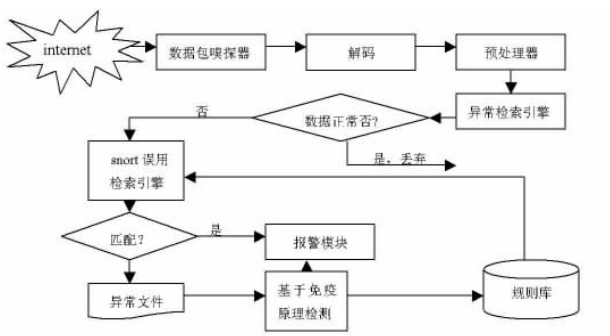

图 3　Snort 基于免疫原理系统结构图

4.3 系统实现

本文改进模型的实现是基于开源网络入侵检测系统 Snort 及

其相关组件的,这些都可以通过互联网免费获得。具体实现过程分为以下几步进行:

1) 在 Windows 系统下部署一个简单的 snort 网络入侵检测系统。用到的主要软件有:Snort、Winpcap、jpgraph、Mysql、Apache、php、ADODB、ACID 等.对这些软件进行合理的安装和配置,构建起一个功能较完善的 snort 入侵检测系统。

2) 将可疑数据存入可疑数据库并对其进行分类, 使新的人侵数据和正常数据分开。这部分通过在 ACID (AnalysisConsole for Intrusion Databases)中加入相应的处理页面来人机交互实现。

3) 利用数据挖掘算法构建正常行为模式库并实现异常检测引擎模块。异常检测引擎模块在 Snort 程序中使用 C 语言来实现。

4) 对异常数据进行向量转换,利用免疫算法对异常入侵数据进行检测,如果是攻击数据则转换成适合 Snort 的规则。这部分使用 C 语言来实现。

5 结束语

该文提出了一个混合型的入侵检测系统,利用 snort 的预处理技术进行异常检测分类过滤掉大量正常数据,提高人侵检测系统的数据处理能力。再利用误用检测引擎检测已知类型的攻击。对于无法确定的攻击则由后续的基于免疫原理异常检测模块做二次检验;该系统可以进行在线的检测工作,可以自动更新规则库,记忆新类型的攻击,灵活性较高,检测性较强。

参考文献:

[1] 宋劲松.网络入侵检测[M].国防工业出版社,2006.
[2] 杨义先,钮心忻.入侵检测理论与技术[M].高等教育出版社,2007.
[3] 郭文忠,陈国龙,陈庆良,等.基于粒子群和人工免疫的混合入侵检测系统研究[J].计算机工程与科学,2007(29,10).
[4] 袁晖.基于 Snort 的入侵检测系统安全性研究[J].计算机科学,2008(35,4).
[5] 盘红华.基于数据挖掘的 Snort 入侵检测模型设计[J].计算机与数字工程,2008(8).

吕秀华(1971-),女,江苏南京人,工程硕士,研究方向:数据库、网络安全及管理工作。

(上接第 6118 页)

图 3 给出了 K=20,M=4,F=256 的 MC-DS-CDMA 系统中, 不同 β 值下,最优化波形与其他波形的平均 MAI 性能对比。注意,这时的载波间距是最优的。同时注意到,虽然最优化波形可以降低 MAI(在任何 β 值下)。但是在 β 很小的情况下,这种减小不是很显著。在 β 很大的情况下,这种减小比较明显。举例来说,当 β=1.0 时,最优化波形比升余弦波形的 MAI 下降了 10%。

图 4 显示了在 β=1.0 时,MC-DS-CDMA 系统中应用不同的波形和最优载波间距通过 AWGN 信道时产生的误比特率(BER)。从图 4 中可以看出,最优化波形优于其他波形,特别在信噪比很大的情况下。在误比特率在 10^{-5} 这个级别,相比于升余弦和奈奎斯特波形,最优小型分别有 2dB 和 1.5dB 的优势。

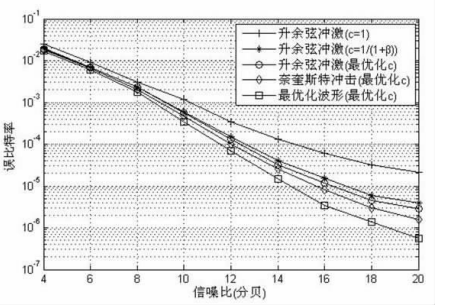

图 4 β=1 情形下,不同波形通过白高斯噪声信道时的误比特率

4 结束语

该文研究了 MC-DS-CDMA 系统中,在载波间距可变条件下,通过最优化波形降低系统平均多址干扰的方法。理论研究和仿真分析表明,这种方法是可行的,并且可以明显降低 MC-DS-CDMA 系统中的平均多址干扰。

参考文献:

[1] R. L. Pickholtz, L. B. Milstein, and L. Schilling, Spread spectrum for mobile communications [J]. IEEE Transactions on Vehicular Technology, vol. 40, pp. 313-322, May 1991.
[2] S. Hara, Overview of Multicarrier CDMA[J]. IEEE Communications Magazine, pp.126-133, Dec.1997.
[3] S. Hara and R. Prasad, DC-CDMA, MC-CDMA and MT-CDMA for mobile multi-media communications[C], Proc. IEEE VTC '96 (Atlanta, U.S.A), pp.1106-1110, April 1996.
[4] S. Kondo and L. B. Milstein, Performance of Multicarrier DS-CDMA Systems[J]. IEEE Transactions on Communications, vol.44, pp. 238-246, Feb.1996.
[5] H.H. Nguyen, Effect of chip shaping on the performance of band-limited Multicarrier CDMA systems [J]. IEEE Transactions on Vehicular Technology, vol.54, pp.1022-1029, May 2005.
[6] S. Sureshkumar, Techniques to reduce multiple-access interference in multi-carrier CDMA systems [D]. pp.20-24, The University of Manitoba(Winnipeg, Canada), August 2005.

陆利刚(1983-),男,江苏通州人,硕士研究生,研究方向:宽带无线通信;

刘金铸(1963-),男,副教授,主要研究方向为移动通信;
倪敏(1984-),女,硕士研究生,主要研究方向为超宽带通信。