文章编号:1004-5694(2005)01-0097-05

基于协议分析状态机的入侵检测系统*

蔡罡[1],冯辉宗[1,2]
(1. 重庆大学 计算机学院,重庆 400030; 2. 重庆邮电学院,重庆 400065)

摘 要:协议分析状态机是提高协议分析正确性的重要保证。将其应用于入侵检测系统是一个新的研究应用方向。协议的形式化描述工具有穷状态自动机、通信有限状态自动机。在此基础上重点讨论了使用协议状态机分析入侵事件的相关算法及流程,设计了基于协议分析状态机的入侵检测系统的总体框架,提出了该状态机的面向对象的模型,使该系统具有良好的可扩展性和通用性。测试结果验证了这一思想的正确性和有效性。

关键词:协议分析;有穷状态自动机;通信有穷状态自动机;入侵检测系统
中图分类号:TP309 文献标识码:A

0 引 言

随着信息技术的不断发展,Internet 已经越来越深入到社会的每一个角落。随着人们安全意识的逐步提高,入侵检测系统(IDS)的应用范围也越来越广,各种各样的IDS 也越来越多[1]。当前的入侵检测系统普遍采用的是模式匹配的思想、模式匹配的算法,但是这样的技术存在着一定的缺陷,主要表现在3 个方面:① 没有考虑到通信协议的特点。在降低了判断效能的同时,对采用连带攻击,数据包分片攻击的方法显得无能为力;② 计算负荷大。对一个满负荷的100 M 以太网而言,需要每秒720 亿次计算;③ 检测准确率低。使用固定的特征模式来检测入侵只能检测特定的特征,这将会错过通过对原始攻击串做对攻击效果无影响的微小变形而衍生所得的攻击。

基于上述方面的原因,人们在实际的应用中越来越感受到采用传统的模式匹配方式已经不能适应网络安全建设日新月异的要求了。于是人们提出了协议分析加命令解析技术,它结合高速数据包捕捉、协议分析和命令解析来进行入侵检测,给入侵检测战场带来了许多决定性的优势:① 提高了性能。协议分析利用已知结构的通信协议,与模式匹配系统中传统的穷举分析方法相比,在处理数据帧和连接时更迅速、有效;② 提高了准确性。与非智能化的模式匹配相比,协议分析减少了虚警和误判的可能性,命令解析(语法分析)和协议解码技术的结合,在命令字符串到达操作系统或应用程序之前,模拟它的执行,以确定它是否具有恶意;③ 进行了状态的分析。当协议分析入侵检测系统引擎评估某个包时,它考虑了在这之前相关的数据包内容,以及接下来可能出现的数据包。与此相反,模式匹配入侵检测系统孤立地考察每个数据包。从通信协议工程学的角度,通过使用协议自动机,探讨使用自动机来对各种协议的状态进行分析,从而达到减少运算规模,提高检测准确性的方法[2-12]。

1 通信协议的形式化描述及相关概念

所谓"协议",在这里指的是计算机网络和分布式系统中各种通信实体或进程间相互交换信息时必须遵守的一组规则,是计算机网络的核心。

协议自动机是网络协议的形式化描述的重要工具。在本文中,我们主要用确定有穷状态机 FSM (finite state machine),或者称为DFA(deterministic finite automata)进行形式化描述。这里我们只对TCP 协议进行分析。

1.1 确定有穷状态机(FSM)

定义 设 X,Y 和 S 是 3 个非空有限集,δ 是笛卡儿积集 $S \times X$ 到 S 的单值映射,λ 是 $S \times X$ 到 Y 的单值映射,则称系统 $\langle X, Y, S, \delta, \lambda \rangle$ 为一个有穷状态自动机。

1.2 通信有穷状态自动机(CFSM)

定义 一个通信有穷状态自动机由一组有穷

* 收稿日期:2004-03-29 修订日期:2004-07-29
基金项目:科技部创新项目(01C26225110726)
作者简介:蔡罡(1978-),男,江苏川沙县人,硕士研究生,主要研究方向为网络安全。

状态自动机的集合 M 和一组通道 C 组成。约定:网络 $N=(M,C)$;$|M|=r$,且 N 满足:

(1) $M=\{m_1,m_2,\cdots\cdots,m_r\}$ 是一个有 r 个有穷状态机的有限集合;

(2) $C=\{C_{ij}:i,j\leqslant r$ 而且 $i\neq j\}$ 是一个通道的有限集合;

(3) 对 M 中的每个自动机 m_i 是确定有穷状态机,其描述与 FSM 定义相同;

(4) C 中的每个通道 C_{ij} 表示 m_i 到 m_j 的通信通道。它是一个先进先出的队列,m_j 从队列的头读出数据作为输入,m_i 把要向 m_j 输出数据送到队列的尾部。

1.3 使用 CFSM 对通信协议进行描述

定义 设一通信协议由一组有穷状态自动机的集合 M 和一组通道 C 组成,约定:网络 $N=(M,C)$;$|M|=r$,且 N 满足:

(1) $M=\{m_1,m_2,\cdots\cdots,m_r\}$ 是一个有 r 个有穷状态机的有限集合;

(2) $C=\{C_{ij}:i,j\leqslant r$ 而且 $i\neq j\}$ 是一个通道的有限集合;

(3) 对 M 中的每个自动机 m_i 是确定有穷状态机,其描述与 FSM 定义相同;

(4) C 中的每个通道 C_{ij} 表示 m_i 到 m_j 的通信通道。它是一个先进先出的队列,m_j 从队列的头读出数据作为输入,m_i 把要向 m_j 输出数据送到队列的尾部。

(5) 对于 m_i,其状态如图 1 所示[13-16]。

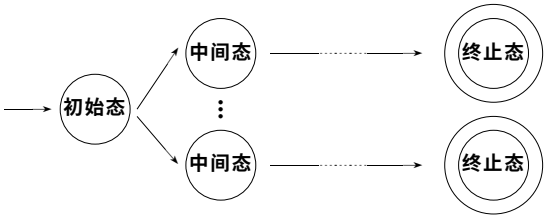

图1 通用协议状态图

Fig. 1 General protocol state chart

2 使用协议状态机分析入侵事件的相关算法及流程

2.1 使用协议状态分析的总体框架

根据以上的分析和描述,以及用状态机对协议进行分析,达到对入侵事件检测的描述,我们可以构建对带有协议状态检测的入侵检测系统的框图,如图 2 所示。

在这个系统中,我们在传统的入侵检测系统的协议捕包和行为检测模块之间添加了一个协议状态检测模块,通过这个模块的工作,我们能通过对协议

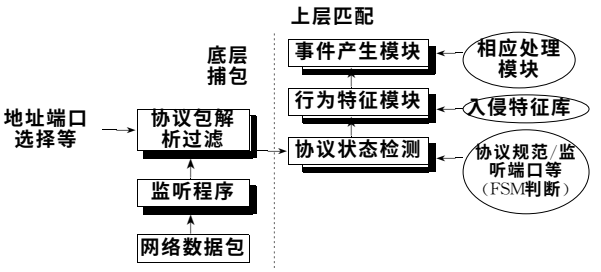

图2 带协议检测的入侵检测系统框图

Fig. 2 Framework chart of an intrusion detection system based on the protocol analyzing

状态的判断达到以下目的:

(1) 防止攻击方使用特征洪水数据包(用以产生大量日志,以淹没少量致命攻击);

(2) 减少对协议非关键阶段数据的冗余检测,以达到提高效率的目的;

(3) 通过对关键阶段的确认与分类,达到智能的对特征匹配发生频率降低,精确度提高的目的。

在这种入侵检测系统的构架下,入侵的特征行为匹配是在状态匹配的基础上进行的。因而,在初始化过程中,我们采用了先构造该有穷状态自动机的状态,后将其特征挂在相应状态下进行。图 3 的匹配

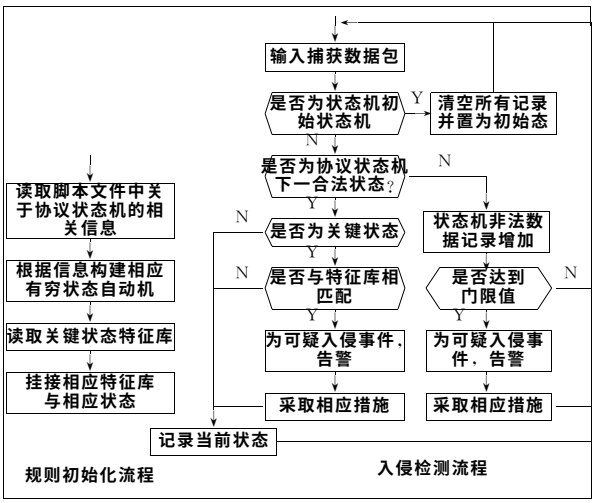

图3 基于协议分析状态机的入侵检测的算法流程

Fig. 3 Flow chart of the algorithm of an intrusion detection system based on the protocol analyzing state machine

方式,充分体现了该基于协议分析状态机的入侵检测系统的构建思想,作为该流程主线上的第 1 和第 2 个判断,能够达到目的(1)中所提出的目标,对该类行为进行记录,并可判断其是否为特征洪水淹没数据包,对这类行为作为一种非法行为加以记录。主线上的第 3 和第 4 个判断,充分体现了目的(2)和目的(3)提出的目标和要求,一方面减少了非关键阶段(如 TCP 的同步和关闭阶段)的冗余检测。另一方面,智能的选择出特征匹配的时机,使得我们对特征的定义也更精确,减少不必要的匹配运算的发生。通过这样的算法安排可较好的降低模式匹配的运算次

数,提高IDS 监测网络的效能和准确度[17]。

2.2 状态检测模块的算法流程

基于协议分析状态机的入侵检测系统的系统初始化及检验算法流程如图3 所示。

2.3 入侵检测系统的面向对象描述

基于协议分析状态机的入侵检测系统的面向对象描述如图4 所示。在一个基于协议分析状态机的入侵检测系统中,我们为每一个通信通道建立一个通信通道对象实例,在该实例中采用了一种AcceptPacket()方法,每一个通信通道对象中包含有一个State 对象的引用。当一个网络数据包被该入侵检测系统捕获到,首先找到其对应的通信通道,并触发该通道的AcceptPacket()事件,在事件的处理过程中,调用State 对象的Handle()方法,并通过不同State 的不同实例,在不同状态下采用不同的处理方式。以下我们将对TCP 协议的具体状态作为例子来做出说明。

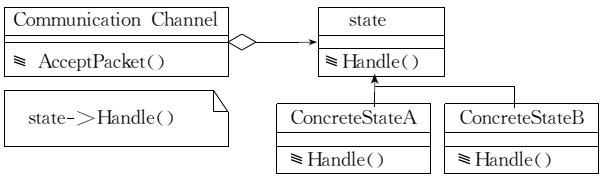

图4 基于协议分析状态机的入侵检测系统的面向对象描述
Fig. 4 Chart of the object oriented detail of intrusion detection system based on the protocol analyzing finite state machine

对于一个TCP 协议的协议状态变迁图如图5 所示,对于每一个TCP 连接,我们均可以做出如图6 的表示方式。

图5 TCP 协议的协议状态机状态变迁图
Fig. 5 Chart of TCP protocol state transition

对于图6 中的Listen 状态,其Handle 事件中的处理过程如图3 中的算法流程图所表示。判断其接收到的数据包是否为其连接的下一状态,即SYN SEND 或SYN RECV 态,若是则将Communication Channel 的状态引用改为相应状态然后对关键状态的入侵行为特征进行匹配,并作出相应动作。对于其他相应状态,以此类推[18]。

图6 TCP 协议的协议状态机UML 图
Fig. 6 UML chart of the TCP protocol state machine

3 协议状态机对入侵事件分析实验

3.1 吞吐量测试

吞吐量测试实验环境如图7 所示,实验结果对照表如表1 所示。在该实验环境中,使用了HUA WEI QUIDWAY S2026 二层交换机作为局域网交换机,实验系统接在该交换机的镜像端口上。从实验数据中可以看出,由于采用了基于协议状态机的包检测方式,该入侵检测系统的吞吐量性能,尤其是在小帧大数据包的情况下,得到了很大的改善,使系统在正常工作状况下的丢包率大大降低,可靠性得到了很大提高。

表1 吞吐量实验对照表
Tab. 1 Data table of throughput test

帧大小	包总数	传统分析包总数	传统分析率%	新系统分析包总数	新系统分析率%
64	148 816	56 818	38.18	119 317	80.19
128	85 414	56 818	66.52	78 837	90.23
256	45 289	45 208	99.82	45 289	100.00
512	23 498	23 452	99.82	23 498	100.00
1 024	11 973	11 973	100.00	11 973	100.00
1 280	9 615	9 615	100.00	9 615	100.00
1 518	8 127	8 127	100.00	8 127	100.00

图 7 吞吐量测试实验环境

Fig. 7 Test environment of the throughput

3.2 时延测试

时延实验环境如图7 所示,结果对照表如表2 所示。从实验数据可以看出,与传统的入侵检测系统相比,该系统由于多了状态机状态检验部分运算,在入侵事件告警的时延性能上与传统系统有所差距,但其反应时间还在接受范围之内。

表 2 入侵事件告警时延实验结果对照表

Tab. 2 Data table of time delay comparison

帧大小	传统分析时延(μs)	新系统分析时延(μs)	新系统反应时延(μs)
64	39.2	39.2	0
128	44.4	44.4	0
256	56.1	56.4	0.3
512	79.4	79.7	0.3
1 024	125.4	125.8	0.4
1 280	145.3	146	0.7
1 518	163.5	164.2	0.7

3.3 误报率测试

误报率实验结果对照表如表 3 所示。从这里的数据不难得出这样的结论,由于对入侵行为特征进行判断以前,有了对协议状态的判断,使得对入侵事件的误报率有了很大的降低。

表 3 误报率实验结果对照表

Tab. 3 Data table of error rate

测试时间(h)	总入侵事件	传统分析误报事件	新系统误报事件
1	10	30	0
4	40	90	0
8	80	200	0
12	120	230	1
18	180	400	3
24	240	600	5

3.4 漏报率测试

漏报率测试结果如表 4 所示,从实验数据可以看出,与传统的入侵检测系统相比,该系统由于多了状态机状态检验部分的运算,在入侵事件告警的漏报率上与传统系统有所差距,但其漏报率还在接受范围之内。

表 4 漏报率实验结果对照表

Tab. 4 Data table of failing to error rate

测试时间(h)	总入侵事件	传统分析漏报事件	新系统漏报事件
1	10	0	0
4	40	2	0
8	80	2	5
12	120	5	6
18	180	5	7
24	240	6	10

4 结 论

综上所述,采用基于协议分析的状态机对入侵事件进行分析,对于解决传统模式匹配的入侵检测系统的计算负荷大、检测准确率低是一种行之有效的方法。我们提出的基于有穷状态自动机的通信信道的描述,也为其他有状态的通信协议或者其他有状态的通信过程都是一种很好的解决方法,这对以后的工作扩展有重要意义。对于这种新的系统,我们在规则的描述上还没有研究,今后需要在这方面着重发展,性能上还存在着漏报和延迟时间的问题,也是在今后需要改进的地方。

参考文献:

[1] ANDREW S. Tanenbaum. Computer networks[M]. Prentice Hall. 1996.

[2] Anderson, JAMES P, Computer security threat monitoring and surveillance[M]. James P. Anderson Co., Fort Washington, Pa., 1980.

[3] HEBERLEIN L. A Network security monitor[A]. Proceedings of the IEEE Computer Society Symposium, Research in Security and Privacy[C]. 1990, 296-303.

[4] DENNING D E. An intrusion-detection model [J]. IEEE Transactions on Software Engineering, 1987, SE-13(2): 222-232.

[5] ALLEN J, CHRISTIE A, FITHEN W, et al. State of the practice of intrusion detection technologies[D]. CMU/SEI-99-TR-028, Carnegie Mellon University, Software Engineering Institute, January 2000.

[6] MCHUGH J. Intrusion detection: implementation and operational issues [D]. Software Engineering Institute Computer Emergency Response Team White Paper, January 2001.

[7] POWER, RICHARD. 1999 CSI/FBI Computer Crime and Security Survey[J]. Computer Security Journal,1999,XU(2): 32.

[8] REBECCA Gurley Bace. Intrusion Detection [M]. Macmillan Technical Publishing, 2000.

[9] PROCTOR, Paul. The Practical Intrusion Detection Handbook[M]. Prentice Hall, 2001.

[10] BACE, REBECCA. An introduction to intrusion detection and assessment: for system and network security management [D]. ICSA White Paper, 1998.

[11] Intrusion Detection and Vulnerability Testing Tools: What Works[EB/OL]. www.sans.org. 2001-02.

[12] 何志国,陈奇. 分布式应用体系结构研究[J]. 重庆邮电学院学报(自然科学版),2003, 15(4):36-39.

[13] LEE D, YANNAKAKIS M. Principles and methods of testing finite state machines-a survey[J]. Proc. of the IEEE, 1996, 84 (8):1090-1123.

[14] LEE D, YANNAKAKIS M. Testing finite-state machines: state identification and verification Computers [J]. IEEE Transactions on,1994,43(3):306-320.

[15] 陶仁骥,自动机引论[M]. 北京:科学出版社, 1986.

[16] C. E. 申南, J. 麦克卡赛. 自动机引论[M]. 陈中基译. 北京:科学出版社,1963.

[17] DOUGLAS Comer E, DAVID Stevens L. Internetworking With TCP/IP Vol: II Design, Implementation, and Internals (Second Edition) [M]. Prentice Hall; 2000.

[18] ERICH Gamma, RICHARD Helm, RALPH Johnsonet al. Design Patterns Elements of Reusable Object-Oriented Software[M]. Addison-Wesley Professional;2000.

(责任编辑:刘勇)

Intrusion detection system based on protocol analying state machine

CAI Gang[1], FENG Hui-zong[1,2]

(1. *School of Computer science, Chongqing University, Chongqing* 400030, *P. R. China*;
2. *Chongqing University of Posts & Telecoms*, 400065, *P. R. China*)

Abstract: Protocol analyzing finite state machine plays a very important role in guaranteeing the correctness of protocol analyzing. Protocol analyzing finite state machine is a new concept in intrusion detection system. In this paper, the authors try to apply protocol analyzing finite state machine to routing intrusion detection system. Authors show the formal models for protocol specifications: finite state machine and communicating finite state machine. And the authors also review the work on intrusion detection system based on protocol analyzing finite state machine on these models, analyse the problems and also show the implementation of intrusion detection system based on protocol analyzing finite state machine. And the authors also introduce, a protocol analyzing finite state machine architecture and analyse the experimental results of the intrusion detection system based on protocol analyzing finite state machine.

Key words: protocol analyzing; finite state machine; communication finite state machine; intrution detection system