插件式网络安全集成防护框架*)

韩 宏 卢显良 任立勇
(电子科技大学计算机学院 成都610054)

摘 要 随着Internet的普及,网络安全问题越来越成为令人关注的问题。单一的入侵检测或者是防火墙系统很难对系统进行有效的防护。如果能整合入侵检测和防火墙形成一种有机的新系统,将能较好地克服两者的缺陷。这里面临了两个问题:一方面需要一种框架能集成新的子系统,即集成入侵检测系统,融合不同的检测技术,同时集成管理不同类型的防火墙,形成结合边界防火墙的分布式防火墙;另一方面需要一种机制,能自动判定入侵检测系统的告警,生成相应的防火墙规则阻断攻击。为了集成不同类型的子系统,我们提出了一种插件式的框架,通过添加插件,它能够集成管理不同类型的防火墙和入侵检测系统,通过该框架的抽象,提供了一种告警自动响应的机制。

关键词 插件式,集成防护框架,入侵检测,防火墙,网络安全

Pluggable Network Integrated Protection Framework

HAN Hong LU Xian-Liang REN Li-Yong
(School of Computer Science,UESTC, Chengdu 610054)

Abstract With the development of internet, the network security becomes attraction. It is hard to be satisfactory if only use separate firewall or intrusion detection system. If we could integrate the two systems we could protect network better. There are two problems: one is that we need to integrate different type firewalls and different type IDS. The other is that the alerts from IDS need analyzing and create relative firewall rules to block attacking. We present a framework that could integrated different type firewalls and intrusion detection systems with pluggin and could collaborate firewall with IDS.

Keywords Pluggin, Integrated protection framework, Intrusion detction, Firewall, Network security

1 引言

入侵检测系统近年来越来越受到重视,但单一的入侵检测系统很难防护不断更新的入侵技术。要从整体上检测入侵行为,单一检测手段远远不够,必须集成各种方法并形成高层次协同互动。Common Intrusion Detection Framework (CIDF)就试图提供一种统一的协议[1]。传统的边界防火墙存在内部不安全、单点失效等问题,研究者试图通过分布式来解决,因此产生了诸如分布式防火墙[2]、防火墙带(farms)[3]、防火墙瀑布[4]等方案。这些方案的背后揭示了一个共同的主题——集成。另一方面,防火墙在被动防御方面性能优越,能及时封闭异常网络流,但其侦测入侵能力十分有限。入侵检测系统探测异常能力较强,但其反击入侵能力有限(基于网络的入侵检测系统一般只能对TCP连接发送RST信号[5])。如将二者结合取长补短,则可完善整体网络防御性能。即:入侵检测侦测入侵后,通过集成系统使防火墙动作,阻止入侵进一步发展。

我们提出了一种插件式集成框架,可集成管理不同类型的防火墙和入侵检测系统,在该框架的基础上,提供了入侵检测告警到防火墙系统的自动响应。以插件方式解决被管理子系统的异构性,必须解决以下四个方面的差异性:1)控制界面的差异、2)控制逻辑的差异、3)存储格式的差异、4)告警通讯格式的差异。该框架应用面向对象技术的多种模式,通过插件对不同类型系统在以上四个方面完成差异性封装,很好地解决了问题。目前系统提出了四种防火墙和三种入侵检测管理的插件。

2 框架结构

2.1 系统结构

该框架由三部分组成:代理、控制中心、命令/消息。

(1)代理:提供具体防御功能,可以是入侵检测、防火墙、综合分析引擎任一技术或复合功能。

(2)控制中心:管理代理并完成代理间协作,包括安全事件分析与反入侵响应、提供分析引擎扩展机制等功能。控制中心可成为其它控制中心管控合作对象。

(3)命令/消息:完成控制中心和代理间协作。命令是控制中心流向代理/控制中心的控制数据;消息是代理/控制中心流向控制中心的数据。

该框架具有良好扩展性、自治性和负载均衡等优势,图1给出了系统一种拓扑结构。

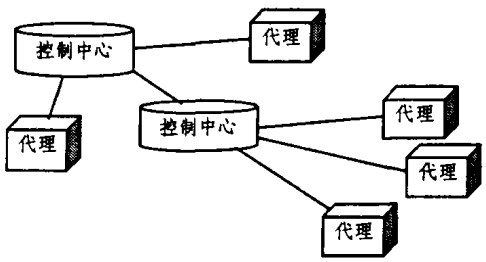

图1 集成平台的拓扑结构

2.2 框架组成

*)本文受信息产业部生产发展基金项目网络安全集成防护系统支持,项目代号信运部[2002]546。韩 宏 博士,主要研究方向:网络安全、软件工程。卢显良 教授,博士生导师,主要研究方向:计算机网络、操作系统。任立勇 博士,主要研究方向:计算机网络、操作系统。

图2为系统框架组成。控制中心功能是代理功能的超集。因此，图2给出的是控制中心的框架。通过裁剪，可得到代理节点的框架。

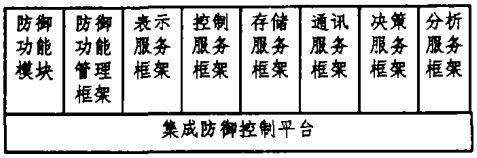

图2 控制中心框架组件

框架分为组件与连接器。防御功能模块为框架组件(Component)，子框架为连接器(Connector)。简述如下：

(1)防御功能模块：插入框架中完成具体防御功能管理的模块，为框架的组件，被集成的对象，例如 Snort 的控制模块。模块由集成系统构造者/第三方实现。通过 Wrap 方式，在未支持统一标准情况下，能集成各种防御技术。防御模块支持表示、消息、控制和存储四个接口，通过它们模块能插入框架。

(2)防御功能管理子框架：该框架管理防御功能模块，提供组件查找、加载和存储管理，并提供运行时组件更新服务。例如显示框架需某防御功能模块控制界面时，向防御功能管理框架提出查找请求并获得该模块的显示接口。

(3)表示服务子框架：提供防御功能模块显示控制服务，包括数据输入和输出。例如为完成某种入侵检测子系统配置，表示服务框架将调用防御功能模块显示接口。表示服务从模块获取输入并提交相关框架。

(4)控制服务子框架：通过调用防御功能模块控制接口，完成对框架节点的控制，其中极为重要的服务是配置服务。

(5)存储服务子框架：对防御功能模块所需存储数据统一管理。常见例子是框架节点配置数据的存储访问。不同类型防御功能模块数据格式是相异的。

(6)通讯服务子框架：提供认证和加解密服务，同时提供消息解析功能和通告机制。另外提供控制命令的通讯模板，通过该模板，控制命令相关通讯和显示及异常处理流程可被复用，最终完成通讯控制的可插入性。

(7)决策服务子框架：支持响应机制与响应策略的分离，实现了响应策略和机制的可插入性。并对插入的响应策略提供了优先级调度能力。

(8)分析服务子框架：提供了扩展异常事件分析的能力。通过插入分析模块，平台可增加新的分析策略，支持更复杂的事件数据融合过程。

图3给出了集成防御平台子框架间调用关系。

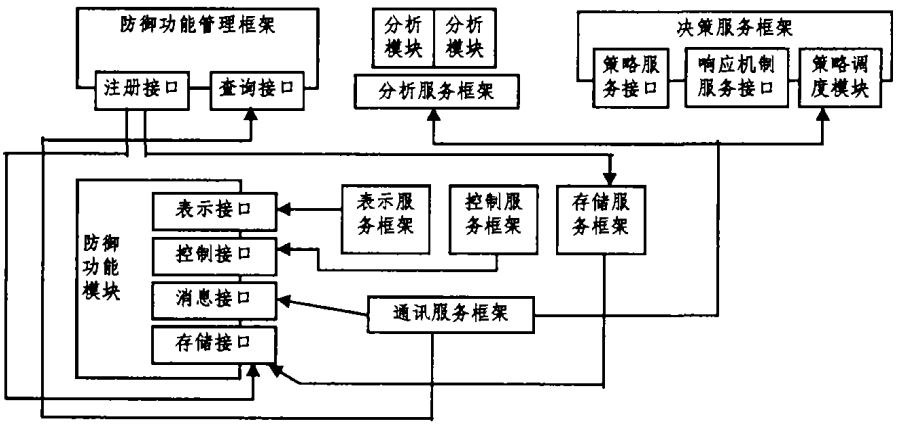

图3 集成防御框架内部交互

2.3 框架交互实例

(1)*防御功能模块注册* 系统添加新防御功能模块时，需调用防御功能管理框架注册服务。该服务调用被注册模块存储接口获取其存储需求，并传递给存储服务框架完成存储定制(例如生成相关数据表)；然后注册服务将存储新添加模块，如图4。

(2)*通讯协议解析* 通讯协议解析及编码必须可动态插入，这里简单地给出了协议解析流程。当网络消息到达时，通讯服务向防御功能管理模块查询相关协议的 Translator，并提交该 Translator 解析。之后将解析结果通知观察者。观察者为分析和决策框架，如图5。

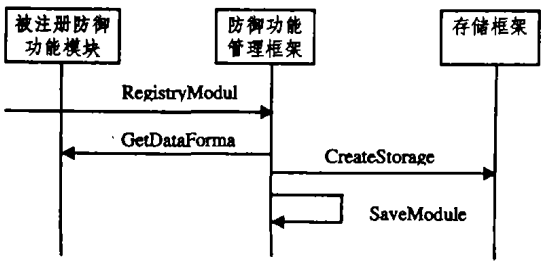

图4 注册新模块

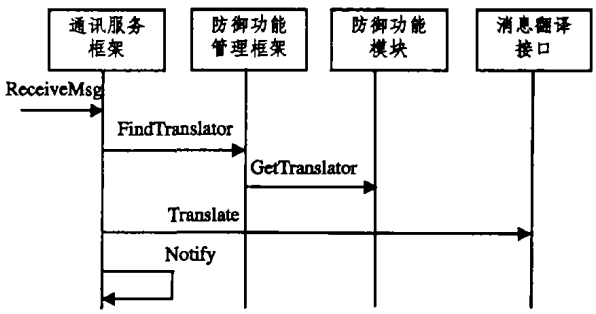

图5 通讯协议解析

2.4 插件的实现

框架中的插件对应图3中的防御功能模块。因为框架和防御功能模块的交互是通过图3中相关的4个抽象接口完成的，所以不同的系统插件，只需要实现对应的接口，就可以插入到框架中运行。有多种方式，支持插件的技术方面，和系统实现方式相关。1)可采用 COM；2)如果是 Java 实现，可采用 Java 的类动态加载技术；3)其它面向对象语言，可采用 DLL 实现

(下转第167页)

采用的是动态规划优化算法这样一个近似穷举搜索(near-exhaustive search)的策略。它生成一个近乎最优的连接顺序，但是可选路径的数目是随着参加链接的表的个数呈指数倍增长的。这样就使得普通的 PostgreSQL 查询优化器不适合处理非常复杂的(参加链接的表数目大于10)的请求。德国弗来堡矿业及技术大学自动控制系的成员在试图把 PostgreSQL DBMS 作为用于一个电力网维护中做决策支持的知识库系统的后端时，碰到了上面的问题。他们提出了一种新的优化策略，这就是基因查询优化。

基因查询优化是基于一种启发式的优化方法 (heuristic optimization method)——基因算法(GA)的，它通过既定的随机搜索进行操作。具体的基因算法请参照文[6]。

在 PostgreSQL 里的 GEQO 实现的一些特性是[2]：

1)使用稳定状态的 GA(替换全体中最小健康度的个体，而不是整代的替换)允许向改进了的查询规划快速逼近。这一点对在合理时间内处理查询是非常重要的。

2)边缘重组交叉(edge recombination crossover)的使用特别适于在用 GA 解决 TSP(旅行推销员问题)问题时保持边缘损失最低。

3)否决了把突变(Mutation)作为基因操作符的做法，这样生成合法的 TSP 漫游时不需要修复机制。

GEQO 模块让 PostgreSQL 查询优化器可以通过非穷举搜索有效地支持大的连接查询。基因查询优化算法采用一种不同于传统优化算法的策略，有着自己不同的特点，将在下一篇论文里作详细的论述。

总结 影响传统查询优化效率的因素主要有以下一些：

1)一个请求中的选择、投影、链接的执行顺序的选择。

2)访问某个关系时访问方法的选择：顺序扫描、索引扫描。

3)链接方法的选择：嵌套循环链接、归并链接、哈希链接。

4)链接顺序：左链接、右链接、布希链接。

PostgreSQL 使用动态规划算法，考虑了这些因素几乎所有可能的组合(路径)，并通过 pg_statistic 中的统计数据来评估每个路径的代价，以选出最优的。

PostgreSQL 中的优化器还实现了其他传统查询优化技术，比如平面化子查询。实现了等价集合的概念，简化了路径的比较。支持基因优化算法，为处理复杂的链接查询提供了可能。本文还提出了对于路径构造算法的一个改进，使其复杂度明显降低。

参 考 文 献

1 PostgreSQL Development Group. PostgreSQL V-7.3.4 source codes. PostgreSQL website http: www.Postgresql.org, 2003

2 PostgreSQL Development Group. PostgreSQL V-7.3.4 Documentation. PostgreSQL website http:www.postgresql.org,2003

3 Ioannidis Y E. Query Optimization Computer Sciences Department University of Wisconsin Madison, 1998

4 Chaudhuri S. An Overview of Query Optimization in Relational Systems. surajitc@microsoft.com 1998

5 Stonebraker M. The design and implementation of the POSTGRES query optimizer http: www.postgresql.org,1989

6 Comp.ai.genetic. The Hitch-Hiker's Guide to Evolutionary Computation

(上接第150页)

插件，将插件的相关接口定义为抽象类(在 C++ 中是纯虚接口)。本系统为 Delphi 实现，采用第三种方式。

3 相关研究

“单个”防火墙的缺陷启发研究者从“协同”与“统一”角度寻找解决方法，即本文关注内容：集成。有以下几种解决办法：防火墙带，它松散布置于物理网络不同位置，由一个管理配置中心和一组位于网络不同物理位置的防火墙组成[3]，该方式未涉及如何集成。分布式防火墙1999年最先由 AT&T 实验室的 Steven M. Bellovin 提出[2]，主要解决了传统防火墙安全拓扑依赖性问题，该方案不涉及防火墙的异构问题，其硬件实现方案被称为嵌入式防火墙[6]。入侵检测领域也有“集成”、“协作”主题的研究，包括：NIDES(Next Generation Intrusion Detection System)[7]、AAFID(Autonomous Agent For Intrusion Detection)[8]等，但它们并未研究中心控制端的可插入性研究。在入侵检测和防火墙协作方面，也未见研究。

结论 本论文提出了一个入侵检测和防火墙的集成管理框架，并讨论其结构和框架的组成，给出了部分框架运作的实例，包括：系统注册、通讯协议解析等。最后给出了插件的多种实现方式。程序的开发实践证明，该框架具有灵活的扩展机制，能够在不修改主程序的情况下，轻松扩展各种被集成系统。而防火墙和入侵检测的协作，也很好地阻断了攻击行为。

参 考 文 献

1 Reilly M, Stillman M. Open infrastructure for scalable intrusion detection. In: Proc. of Information Technology Conf. IEEE, Sep. 1998

2 Bellovin S M. Distributed Firewalls. login: magazine, special issue on security, Nov. 1999

3 Stout B. Firewall Farms Whitepaper. www.geocities.com/ResearchTriangle/3372/firewall farms.html

4 Simth R N. Firewall Implement In A Large Network Toplogy. In: Proc. IEEE Future Trends of Distributed Computing Systems, Oct. 1997

5 Snort2.0 Detection Revisited. http://www.sourcefire.com/technology/whitepapers/sf_snort20 detection_rvstd.pdf

6 Prevelakis V. Designing an Embedded Firewall/VPN Gateway. http://www.prevelakis.net /Papers/vpn8.pdf

7 System Design Document: Next-Generation Intrusion Detection Expert System:[Report]. March 1993

8 Balasubramaniyan J S, Garcia-Fernandez J O. An Architecture for Intrusion Detection using Autonomous Agents: [COAST Technical Report]. June 1998