第30卷 第14期 计 算 机 工 程 2004年7月
Vol.30 № 14 Computer Engineering July 2004
·开发研究与设计技术· 文章编号：1000—3428(2004)14—0187—02 文献标识码：A 中图分类号：TP393.08

基于Snort和Acid的协同入侵检测系统设计与实现

伍 星，唐正军，单蓉胜，童志鹏
(上海交通大学信息安全工程学院，上海200030)

摘 要：提出一种基于Snort和Acid的分布式协同入侵检测系统(SADIDS)，控制台和传感器之间传送的控制命令用SADIDS命令格式编码，添删的规则用Blowfish算法加密，使传感器之间的工作既具有独立性，并且通过远程配置，又可以使各个传感器之间安全地进行最大可能的分工协作，系统组件功能的独立均衡保证了自身的安全性。

关键词：入侵检测；协同；分布式；远程控制

Design and Implementation of Cooperation Intrusion Detection System Based on Snort and Acid

WU Xing, TANG Zhengjun, SHAN Rongsheng, TONG Zhipeng
(School of Information Security Engineering, Shanghai Jiaotong University, Shanghai 200030)

【Abstract】 This paper describes the design and implementation of co-operation intrusion detection system based on Snort and Acid (SADIDS). The control commands communicating between console and sensor are encoded with SADIDS command format. The adding or deleting rules are encrypted with Blowfish algorithm. This measure ensures the independence of the work and the most impossible safe co-operation among sensors. The independence and equilibrium of the system modules ensure the security of SADIDS system.

【Key words】 Intrusion detection; Cooperation; Distributed; Remote control

随着系统漏洞的交流和攻击工具的传播，分布式环境下的协同攻击与日俱增，然而传统的IDS局限于单一主机或网络架构，不同的IDS系统之间不能协同工作。为解决这一问题，多级互动的分布式协同入侵检测技术与通用入侵检测架构应运而生。最先出现的分布式IDS利用分布在网络中的传感器扩大了数据源的范围，但最终的数据分析却是集中进行的。这样做带来的问题有两个：一是整个系统有一个中心控制点，该点的失效将导致整个系统失效；二是集中进行数据分析使负载集中在承担分析工作的主机上，限制了系统的可扩展性与效率的提高。

对于集中控制的分布式IDS的弊病，无控制中心的方案是突破瓶颈的方法。为此本文提出一种基于Snort和Acid的分布式协同入侵检测系统(SADIDS)的设计框架，并且通过php和vc的混合编程实现控制台和传感器之间的远程交互。单个传感器是基于Snort的，本身具有数据采集，入侵分析、响应的功能；单个传感器把分析结果上传给所属域的基于php的控制台Acid，由控制台统一管理警告信息，并图形化分类显示，这个域的管理员可以根据当时的情况和网络需求在控制台远程控制各个传感器(Sensor)。控制台和传感器之间传送的控制消息用SADIDS编码格式编码，规则添删消息用Blowfish[1]算法加密，这样一来，传感器之间既具有独立性，并且通过远程配置，还可以使各个传感器之间安全地进行最大可能的分工协作[2]。组件本身的功能不再是影响整个系统的关键因素，也就是说，一个组件失效仅仅使整个系统的能力降低，而不会使整个系统失效。系统的结构相对固定，而系统各组件何时该独立工作，何时需要协作则相对灵活。通过灵活分配角色的协作机制，能够更准确地反映出分布式各个组件之间的关系，具有更大的适用性。

1 SADIDS分布式协同入侵检测系统的基本结构

基于Snort和Acid的分布式协同入侵检测系统是多级协同交互的分布式体系，其二级系统结构如图1所示。在最高级别上，SADIDS分为两个子系统：本地入侵检测子系统，集成网络管理子系统。

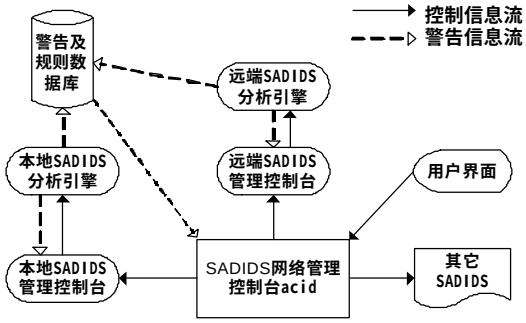

图1 SADIDS协同入侵检测系统结构

1.1 本地入侵检测子系统

作为底层实体，本地入侵检测子系统负责收集数据、分析数据，将分析结果报告给所属的管理控制器。基于Snort的本地SADIDS分析引擎首先对各种协议栈上的数据包进行解析、预处理，例如对报文进行分片重组、流重组和异常检测等预处理工作，以便提交给检测引擎进行规则匹配；接着将解析后的数据包与已存储的检测规则进行递归匹配，当数据包满足一个规则时，就触发相应的操作，例如日志记录或报警；然后将告警信息发送给本地SADIDS控制台和系统警告与规则数据库。每个入侵检测子系统可以根据自己收集的数据在本地控制模块上先进行分析，以便做出实时决策。

1.2 集成网络管理子系统

基金项目：国家“863”计划基金资助项目(2001AA140214)；武器装备预研基金资助项目
作者简介：伍 星(1980－)，女，硕士，研究方向：网络与信息安全；唐正军，博士后；单蓉胜，博士；童志鹏，院士
收稿日期：2003-06-26 E-mail：wu-xing@sjtu.edu.cn

集成网络管理子系统是基于php的Acid Web管理平台。控制台所完成的功能包括：触发安全规则的网络流量中各种协议所占的比例、警报的数量、入侵主机和目标主机的IP地址及端口号等。此外，SADIDS控制台还提供远程控制、规则配置功能和强大的搜索功能，用户可根据时间、IP地址、端口号、协议类型以及数据净荷(payload)等多种条件的灵活组合，在入侵事件数据库中进行查询，远程对Sensor发送控制命令，如迅速启用协同机制，自动通知防火墙或其它安全控制设备切断攻击源，配置规则等来帮助管理员进行分析和网络整体安全的管理。同时，集成网络管理子系统可以通过各个网段上Sensor发送到警告及规则总数据库的警告进行协同分析，基于复杂精确的协同算法，进行数据挖掘，状态转移预测做出更正确的决断。

2 实现

基于Snort 和Acid的分布式协同入侵检测系统SADIDS，实现了远程控制的功能，例如能对远端SADIDS系统内主机发送所有Snort和Nmap支持的命令，并能远程关闭和重启分析引擎，对指定的Sensor远程配置适合当时情况的规则。这样，集成网络管理子系统通过对全局网络信息的分析，让每个SADIDS分析引擎提高实时检测能力和安全防护能力。

2.1 SADIDS网络管理控制台

控制台是用php实现的基于Acid的管理组件，两大功能是对控制消息的编码和发送、对远端Sensor的规则配置。

(1)实现控制消息传送的基本思想是定义一套支持Snort和Nmap所有命令的32b编码，通过基于TCP的可靠连接远程发送给已注册的指定Sensor，指定Sensor收到后发给总控制台一个确认信息，至此，控制命令的通信结束。

首先，定义控制消息的编码格式。明文传送是非常危险的，一旦第三方获取消息，并进行篡改，就可以获得对系统分析引擎的控制权，所以必须约定SADIDS管理控制台和分析引擎的通信格式来保证各个组件之间安全、高效的通信。也就是说，要实现有目的的通信，各组件就必须能正确理解相互之间传递的各种数据的语义，编码的任务就是提高组件之间的互操作性，所以命令消息的组成结构就如何表示各种各样的事件做了详细的定义，格式如图2所示。

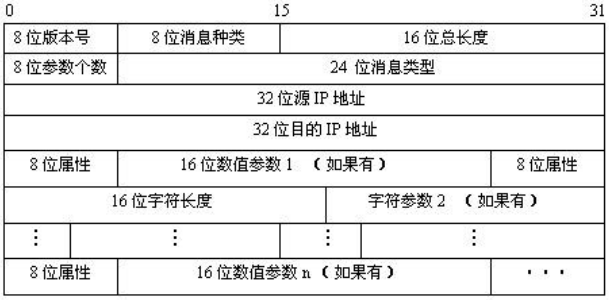

图2 SADIDS 命令消息的编码格式

注：最高位在左边，记为0 bit；最低位在右边，记为31 bit；版本号目前为1；命令种类是指Snort，Nmap命令；参数个数是指本返回的确认消息所带参数的个数；消息类型是指此命令消息在所属消息种类中的类型；总长度是指命令编码后占用内存的字节数；属性是指参数是数值型还是字符型，0为数值型，1为字符型；字符长度是指如果参数是字符型的，占用内存的字节数。

(2)实现SADIDS管理控制台的远程规则配置功能。当某个Sensor发生入侵时，如蠕虫病毒，DdoS攻击等，中央控制台可以对系统内注册的Sensor远程配置规则，在其规则库中加入新规则来阻止攻击行为扩散，而不需要将Sensor停下来，在每个入侵检测子系统上人工配置规则；当需要对规则进行升级，剔除不实用的旧规则时，也可以远程删除。远程规则配置的基本思想是：

1)中央警告及规则数据库存储整个系统的规则，当需要修改某个Sensor的规则时，找到Sensor在主控制台上注册的编号就可以对其规则进行增删；

2)主控台记录注册Sensor规则的Mysql库表元组rules(sid, sensor, alerttype, protocol, route, msg)。SADIDS主控台对Sensor规则的添、删是通过rules元组中的Sensor做标记位决定的。也就是说，在数据库中并不是根据每个注册的Sensor存储规则，而是对某个特定规则而言，用32b标志位来标记规则所属的注册主机，比特位由低到高表示注册主机的先后顺序，例如，当前规则属于Sensor1、3、5，则这个规则Sensor一项的值就记为21，即10101。这样设计的优点可避免同一条规则在主控台数据库中重复存储，避免数据冗余。

3)发送给指定Sensor添加删除的规则消息用Blowfish算法加密，Blowfish 将64 b的明文分组加密为64 b 的密文分组，然后用Socket发送给指定Sensor，如果指定的Sensor接收到消息，并完成相应操作，则返回给主控台一个确认信息。

2.2 SADIDS本地入侵检测子系统

SADIDS的本地入侵检测子系统设计的基本思想：基于Snort，并加入Nmap进行入侵检测的先期扫描，防守的同时主动进行扫描察看网络系统的主机分布以及其上运行的服务种类，达到知己知彼，百战不殆。SADIDS本地入侵检测子系统在接到管理控制台发送的远程控制命令后，先根据图2的消息编码格式进行解码，然后在本地入侵检测系统中执行；当接收到远程配置的规则消息时，根据Blowfish分组密码算法解密，并在本地规则库添加/删除相应规则。

3 结论与展望

论文实现的SADIDS协同分布式入侵检测系统由中央控制台负责管理各个分布的Sensor协同工作。由于各个Sensor具有独立分析的功能，就不会形成瓶颈，一个Sensor的失效，不会导致整个系统的瘫痪，系统所受的影响只是局部入侵检测性能的降低。中央控制台的远程控制命令、配置规则功能，保证对系统全局的入侵行为做出快速反应，消息的编码格式与Blowfish加密算法保证了主控台与Sensor的通信安全，对规则标志位的加入，防止了数据冗余。

对SADIDS系统的一个设想是把它做成基于硬件的入侵检测系统[3]。因为软件实现的分布式协同入侵检测系统有两个与生俱来的缺点：第一，随着网络被保护主机的增加，引入了高带宽数据传输所不能容忍的通信时延；第二，一旦入侵者获取了系统权限，也就获得了操作入侵检测软件的权限，主控台的远程控制功能更方便入侵者控制整个网络。所以，尽可能地用硬件实现入侵检测系统的功能是SADIDS的一个发展方向。

参考文献

1 Stallings W.Cryptography and Network Security.Principles and Practice Second Edition,1999

2 Buchheim T, Erlinger M, Feinstein B. Implementing the Intrusion Detection Exchange Protocol. Computer Security Applications Conference, 2001

3 White G B, Huson M L.A Peer-based Hardware Protocol for Intrusion Detection Systems. Military Communications Conference, 1996,2: 468 -472