网络防御和不重复子串模式匹配算法研究实现

陈伟东[1,2],黄祖泉[1],陈传波[2],张伟平[1],吴 涛[2]
(1. 上海颐东网络信息公司,上海 200233;
2. 华中科技大学 软件学院,湖北 武汉 430074)

摘 要:云计算网络和下一代网络技术的广泛应用,带来了更多安全威胁。文中基于进程和网络元组,研究实现了网络主动防御系统的关键技术。研究了 IPv4/IPv6 双协议栈网络体系下防御关键技术,提出了基于最长不重复子串和 Sunday 算法的改进算法—NRLS_Sunday,避免了对重复字符过多比较,提高了单模式字符串的匹配效率。与 BM、Sunday 算法的效率作了实验对比,优化了算法的时间复杂度。研究了在高速网络下,快速对数据包做内容检测和分析的方法。采用基于进程和网络元组的网络智能流量限制,对网络做入侵检测和防御。研究了在高速网络要求下对网络做并行检测方法。在复杂网络空间环境下应用网络协作,统一部署和下发策略,提出和实现了在复杂网络环境下防御的有效方法。

关键词:网络防御;系统内核;网络安全;最长不重复子串;改进的 Sunday 算法
中图分类号:TP301 **文献标识码**:A **文章编号**:1673-629X(2016)07-0089-05
doi:10.3969/j.issn.1673-629X.2016.07.019

Research and Implementation of Network Active Defense and Pattern Matching Algorithm

CHEN Wei-dong[1,2], HUANG Zu-quan[1], CHEN Chuan-bo[2], ZHANG Wei-ping[1], WU Tao[2]
(1. Yidong Network Information Co., Ltd, Shanghai 200233, China;
2. School of Software Engineering of HUST, Wuhan 430074, China)

Abstract: Cloud computing network and next-generation network is now widely used, which brings more security threats. Based on the process and the network tuples communication to construct defense system, the key technologies of defense under IPv4/IPv6 dual stack network are researched. It presents the NRLS_Sunday based on improvement of the longest norepeat substring and Sunday algorithm, to avoid excessive repetitive character comparison and improve the matching efficiency of a single pattern string. Compared with BM, Sunday algorithm, the experiment shows the improved algorithm optimizes its time complexity. Under high-speed network, packet data contents is carried on rapid detection and analysis. Based on intelligent traffic restrictions for process and network, the intrusion detection and defense is conducted for network. In this paper, parallel packet detection method is studied under the high speed. Application web collaboration, and the unified arrangements and issued policies is applied in a complex network environment, proposing and realizing the effective method of defense in the complex network environment.

Key words: network defense; system kernel; network security; the longest norepeat substring; improved Sunday algorithm

1 概 述

云计算的逐渐普及带来了安全和隐私的风险。分布式的存储和并行计算在带来方便快捷的同时,也对网络安全存储和相关的业务活动带来了泄露和损坏的可能。下一代网络体系(IPv4/IPv6)存在已知和未知的各类安全威胁。规模网络的云计算平台,应用虚拟化技术和云存储等免费带宽等服务,对网络入侵的防御、审计取证和有效预防成为保障云环境安全的重要措施。

云计算资源包括数据中心服务器、分布式研发平台、存储设备等。数据中心网络的大量部署,虚拟计算和分布式存储、分布式计算给网络安全带来了新需求。需要提供从系统行为监控到网络监控的一体化解决方案。云计算安全威胁包括:数据泄漏、系统漏洞、个人认证信息丢失、加密密钥丢失;文件加密信息泄漏;客户私钥、数据丢失:会话劫持、Web 入侵、拒绝服务攻

收稿日期:2015-09-14 **修回日期**:2015-12-17 **网络出版时间**:2016-05-25
基金项目:国家自然科学基金面上项目(51175197)
作者简介:陈伟东(1970-),男,硕士,高级程序员,系统分析师,CCF 会员,研究方向为系统网络安全。
网络出版地址:http://www.cnki.net/kcms/detail/61.1450.TP.20160525.1708.044.html

击 DoS。如采用 80 端口的僵尸网络 DDoS 攻击难于检测和防御,混合了 HTTP 和 XML 消息试图毁坏云服务提供者通信信道流。云计算存储、虚拟化和资源管理等方面都需要安全保证。

僵尸网络发作和传播采用的方式十分隐蔽,如较流行的 TDL 系列。采用的 P2P 的分布式网络,利用域名生成算法(DGA)与 C&C 服务器通信。僵尸网络采用底层驱动隐藏自身,难以检测。需要在网络通信层面对通信做检测和拦截,根据协议状态的匹配和异常通信等发现可疑通信数据。APT 类型的攻击(高级持续性威胁)利用各种手段感染目标网络,利用 C&C 服务器通信,造成企业关键信息泄漏。

云计算网络一般采用分布式文件系统,虚拟化技术、分布资源管理、并行计算编程模型(MapReduce 等)。数据存储采用分布式数据存储,对海量非结构化数据可以并行读写和高效率存储与访问。如 GFS 是可伸缩的分布式文件系统,利用控制消息和数据消息做规模运算。

在入侵检测和防御系统方面,对模式匹配的速度决定了网络速度的瓶颈[1]。对规则模式的高效匹配算法的要求越来越高,对网络通信的检测和取证,可以利用协议状态的转换。建立状态转换图,有效控制利用协议漏洞的 DDoS 攻击。入侵检测结合采用分布式网络防御系统(NIPS)。利用语义规则方法可检测网络协议从驱动层到应用层的异常检测。

对网络内容的快速检测,需要有快速的规则匹配算法。文中参考 Sunday 算法,提出一种根据最长不重复子串来对网络快速匹配的算法。通过实验比较,时间复杂度和跳转次数优于传统的 Sunday 算法。避免了重复字符串比较过多的问题。

2 下一代网络防御技术分析

传统的防御技术主要有基于网络的入侵检测(NIDS)和基于主机的网络防御(HIPS)、在客户端和边界做防御控制等方法。在云计算网络内,对未知文件数据提交到云端作分析和全面检测。对网络 QoS 作控制,对系统建立漏洞数据库、针对系统漏洞做防御,对网络数据处理做深度检测,生成智能规则和防御图等。国内外研究者采用攻防博弈模型、深度数据包检测、基于协议分析和通信异常等发现网络可疑通信。基于神经网络的入侵检测等方法,Schneier 较早(1999)提出了攻击树分析模型,对网络通信的发作环节进行分析和判断。Dacier 采用特权图理论对网络进行检测。应用正则表达式进行规则检测。

IPv6 网络协议栈除了对 TCP 序列号等攻击失效外,大部分传统的 DDoS 攻击仍然有效,DDoS 攻击已覆盖网络栈多个层次,从网络层、传输层到应用层[2]。在下一代网络 IPv4/IPv6 的双协议栈的多个层次,从网络传输层到应用层做立体防范。结合入侵防御等多项技术,才能构建可信的网络防御系统。网络海量数据采用模糊决策树、神经网络等判断异常流量数据。采用攻击图和关联图等技术,根据网络攻击的特征如对网络漏洞的攻击(如 RPC/DCOM 缓冲区溢出),做统一部署和防御。对网络漏洞采用禁用和告警等机制,利用流量检测 DDoS。选择网络元组计算熵值,与正常情况熵值对比,可发现高速和低速 LDoS 攻击。

对协议漏洞如 TCP 的 Syn 连接漏洞、拥塞机制和窗口限制等的 DDos 攻击,网络安全要求对系统漏洞、应用层缓冲区溢出做全面防范等。需要在应用层或网络层应用入侵检测技术[3]。在目前的高速网络环境下,低速 DDoS 攻击利用 TCP 拥塞控制漏洞,可以穿透多数入侵防御系统。HTTP-Flood DDoS 攻击向服务器发送大量的 HTTP GET 数据包请求,占用带宽少,普通的网络防御难以发现混杂在正常流量内的攻击数据包。对 IP/TCP 协议族利用相应头等信息建立 HMM 模型(隐马尔可夫模型)。根据网络语法判断通信是否异常。针对不同网络协议采用不同的防范方法。对于 TCP 有状态协议,可以对 QoS(服务质量)做控制。

对网络数据的深度内容检测多数采用多模式规则匹配算法。多关键字模式匹配算法主要有:AC_BM 算法、WU MANBER 等[4]。开源的入侵检测系统 Snort 部分使用了 AC_BM 算法,在模式检测花费整体运行时间的 70% ~80%。采用模糊测试方法,找到网络协议存在的协议、缓冲区溢出等漏洞。网络协议分析技术把网络攻击提取出状态转换特征,基于有限状态机做检测和报警等。建立状态转换模型。基于网络链接建立状态转换链表,可以在网络层建立协议状态链表,通过对通信 IP 的简单 Hash 确认状态。如针对 TCP 协议的 SYN Flood 攻击的防御方法是:以对此类连接计数并建立队列,当连接数和时间等参数到阈值,丢弃此类连接。

开源的 Snort 系统可以执行实时流量分析和网络数据包日志记录。对通信协议作分析、内容检测和匹配。匹配算法采用基于自动机的多模式查找算法等。Snort 内置规则包括针对缓冲区溢出、网络探测和对协议漏洞攻击等。

Honeypot(蜜罐)技术利用系统或网络漏洞,对黑客行为作诱骗。对 0Day 漏洞,基于网络多元组、时间和事件类型等构成有限自动机作入侵识别。建立漏洞数据库和漏洞扫描机制。系统需要在高速网络运行。利用多队列 NIC 网卡,多 CPU 和多 GPU 结合的方法

提高检测速度,减少网络瓶颈。Gnort 采用 CPU+GPU 做分布并行网络检测识别。硬件可以采用多队列网卡,可以有效提高网络 QoS 性能。将多个网络队列转发到不同的 CPU 上。部分网络检测系统采用 GPU 的运算能力对规则模式做并行匹配。

3　模式匹配算法研究

Snort 系统规则集主要有 Web 规则、缓冲区漏洞规则、扫描和网关攻击防御规则等[5]。传统的 Snort 规则集使用了两维规则链表,分为 RTN(规则头树节点)和 OTN(内容选项树节点)两部分。把网络数据文件收集后,分为两个部分。分别作并行字符串检测。入侵检测系统在网络层取到封包之后,对数据包头作解析,对内容作检测。基于有限自动机检测网络异常。采用多模式字符串匹配算法和并行技术等[6],对数据作多维关联分析。基于云的威胁防御分析,提高匹配效率和对网络大数据的处理。

常用的单模字符串匹配算法有 KMP、BM 等,多模式匹配算法有 AC 和 WU MANBER 等。从性能比较来看,单模式 Sunday 算法在查找速度比较占据优势。Sunday 算法对主串比较末位字符下一位字符,找到在规则串最右出现的位置,做快速跳转。文中提出一种改进的 Sunday 算法—NRLS_Sunday(No Repeat Longest Substring),利用规则字符串的最长不重复字符串。借助 Sunday 算法和最长不重复字符串的特征,能够更快实现规则跳转。Sunday 算法最坏时复杂度为 $O(n*m)$。

文中提出了对规则模式首先找到最长不重复子串的算法,避免了字符的重复比较和频繁移位。对单模式字符串匹配而言,首先找到模式字符串的最长不重复子字符串。最长不重复子字符串能反映规则的性质,避免重复子串造成无意义的比较和跳转次数。

字符串匹配的流程如下:

(1)预处理首先计算最长不重复字符串。然后需要计算两个坏字符数组,一个是规则串本身的坏字符数组 BadChar1[ ],另一个是最长不重复字符串及其之前字符串的坏字符数组 BadChar2[ ]。

(2)开始比较规则字符串的最右一个字符,相等则到 3,不等则比较主串的末位和末位下一位字符坏字符数组值,在两个值中取最大值跳转(参考 Sunday 算法的跳转规则)。

(3)在末位字符相等的情况下,对最长不重复字符串从右到左对规则字符串做顺序匹配。匹配则到步骤 4,失配时跳转规则取 BadChar2[c]和 BadChar1[末位加一]的值的最大值做跳转。

(4)最长不重复字符串及之前的字符已匹配,则比较最长不重复串之后的规则字符。匹配则输出,失配的跳转规则取 BadChar1[末位加一]和最长不重复字符串的长度的最大值做跳转。最少可以跳转最长不重复字符串的长度。

预处理首先要计算模式串的最长不重复字符串,之后需要计算最长不重复字符串到模式首位字符的坏字符数组和规则字符串的坏字符数组。跳转规则可按如下计算:

算式 1:首先比较模式 p 末位字符(c_1),失配则计算

$$Skip = MAX(BadChar1(c_1), BadChar1(c_2))$$

c_2 为规则串对应主串末位的下一位字符。

算式 2:最长不重复子串及之前比较失配时

$$skip = MAX(BadChar2(c_1), BadChar1(c_2), Len)$$

skip 为跳转距离,BadChar2 计算失配字符 c_1 跳转,BadChar1 计算末位加一 c_2 字符跳转。如果比较移位数已超出最长不重复子串长度(Len),则最少移动不重复子串长度。有 skip = Max(skip,Len) 。

算式 3:最长不重复子串及之前字符匹配,在子串后面匹配失效,则跳转规则为

$$skip = MAX(BadChar1(c_1), Len(\text{最长不重复子串}))$$

skip 为跳转距离,BadChar1 计算末位加一跳转,Len(最长不重复子串) 是该串长度。

预处理时计算 BadChar1(坏字符规则)数组、BadChar2 数组和最长不重复字符串。要计算字符串的最大不重复子串,采用动态规划的复杂度是 $O(n^2)$。查找的时间复杂度是 $O(n)$。在字符串左面与模式串对齐,比较时从模式串末位进行。

该算法适用于对较长规则串的查找检测,方法如图 1 所示。

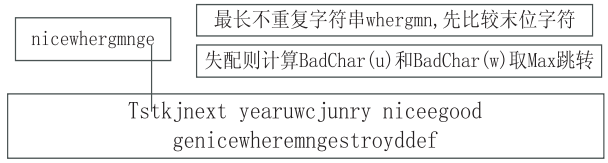

图 1　利用“whergmn”做第一次匹配

从图中可看到,whergmn 为最长不重复串,末位字符‘e’对应‘u’。失配后计算 BadChar1(w)和 BadChar1(u)的值,取最大值做跳转。规则串整体移动到 u(坏字符)之后,如图 2 所示。

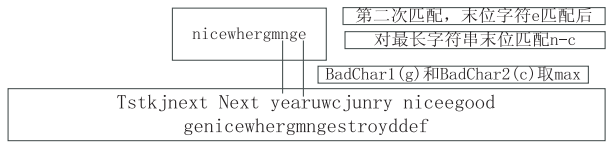

图 2　第二次匹配图

从图中可以看到,尾部字符‘e’相同。则比较最

长不重复子字符串‘n’对应‘c’,计算 BadChar1(g)=2 和 BadChar2(c)=8,则跳转值为 8。

如图 3 所示,‘e’对应‘n’,则计算 BadChar1(i)=12,字符串移动 12。

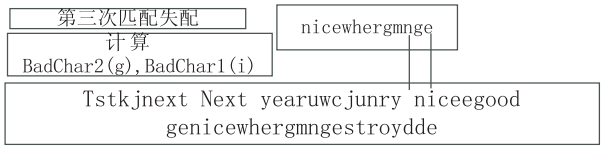

图 3　第三次匹配图

匹配结果如图 4 所示。

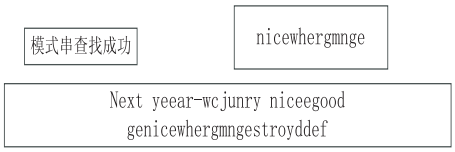

图 4　第四次位移,找到规则字符串并输出

如图 5 所示,如果不重复子串后面失配,则取不重复子串长度和 BadChar[末位加一]的最大值跳转。

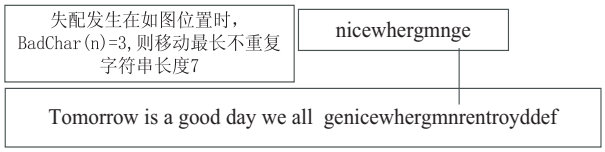

图 5　不重复子串后面失配则移动不重复子串长度

采用该算法可在比较时跳跃最多字符(规则模式串从左向右移动)。算法最大时间复杂度为 $O(n)$,最好情况是 $O(n/m)$。用改进的 Sunday 算法与 BM 算法和 Sunday 算法做查找时间和次数的分析比较时,性能指标如下:

测试环境为 Windows 7 系统,CPU 为 4 核 2.40 GHz,内存 6 G 平台。随机采用一个几十 k 的文本字符串文件,算法利用最长不重复子串和最末位字符作移动,带来了更大的平均移动速度。

算法跳转次数比较见表 1。

表 1　不重复子字符串改进算法跳转次数比较

规则字符串	不重复字符串改进算法	Sunday 算法	BM 算法
Jsdfeskdfcksejdf	16	21	17
aaxbbxa	27	31	29
eskdfcksejdfsdfdsfe	10	15	11
abcdaa	23	25	27
baaasdfs	17	17	21
kjskdfcksejs	12	15	13

从表 1 可以看出,文中提出的算法跳转次数明显少于 Sunday 和 BM 算法,程序时间也保持在此比例。比较 Sunday 算法平均提高 10% 左右的性能。算法的空间性能也没有太多消耗,只是多计算了最长不重复子字符串的坏字符数组。没有计算好后缀数组。平均移动不小于重复子串的长度。快速完成比较。对多模式字符串比较,可采用 AC 算法与文中算法结合的方法。采用 AC 算法构建规则树,采用规则树一次对要对比的规则做模式匹配。

4　云计算网络防范设计与实现

云计算网络首先是对 IP 双协议栈进行异常检测和防御。下一代网络对 IPv4/IPv6 协议栈兼容。网络吞吐量和异常流量检测是确保服务器安全的重要措施。利用系统进程的网络数据流量,对 IP 协议做智能控制。也可以采用主动发包探测网络状况和网卡嗅探器(Sniffer)等,实时监控网络状态。在内容检测方面,模式规则匹配速度很关键。模式匹配算法对存储空间和匹配速度有较高要求。在应用层对网络数据的检测更稳定并具有较好的运算能力[7]。

IPv6 协议集成了 IPSec 对数据加密,Windows 提供了 WFP 驱动(Windows Filtering Platform Drivers)可以在 IPSec 加密前和解密后采集到数据,仍然可以对网络数据做内容检测[8-9]。部署基于主机的 HIPS 系统可以有效对网络数据进行检测和防御。在云计算环境下部署恶意行为检测和防御系统。对 APT(高级持续性威胁)入侵在网络层和文件系统层面做有效检测和防御。网络监控防御和反恶意软件等模块在云计算数据中心部署,对下一代网络协议 IPv6 状态和语义做基于有限自动机的分析。分布式客户端向云端分析服务器传送可疑通信数据和文件等。在虚拟机和主机等构建可信安全的防御体系。采用 WFP 技术对 HTTP 协议流进行数据检测,可以检测禁止信息、未知程序运行等。

最有效率的方法是基于进程和网络元组的网络检测和防御方法。对分布网络节点应该采用不同级别的规则和检测模式。向云端提交可疑通信数据等以作分析。基于网络和主机的 IDS,正常的网络有固定的状态转移图和语法规则,可以用来进行对网络通信异常行为的检测[10]。可使用 GPU 和 CPU 结合对采集到的网络数据做并行检测。将规则置于关键字树之上,采用上文提到的算法检索。对于多模式匹配需要建立规则树。对于采用 0Day 感染系统的安全威胁,在及时更新系统漏洞的同时,需要检测出相应的系统和网络异常。入侵检测方法主要有基于文法的意图识别,根据网络数据上下文信息,采用状态自动机、基于有向无环图或树对属性作匹配,利用有向树因果关联关系,对攻击做报警和检测[11]。

图 6 展示了网络防御系统的总体功能图。

根据系统漏洞和权限等信息构建攻击图。通过漏

洞收集建立模式库,将系统脆弱点转化为攻击关联图。根据深度优先或广度优先对各类攻击模式建立攻击图,完成对网络安全性的评估。对云数据中心服务器作流量控制,对服务器连接 IP 和网络数据流做控制。通过检测丢包率,控制网络带宽和质量,有效控制 QoS(Qulity of Service)。系统通过对网络层和应用层做基于 IP 元组的控制,对内容作有效检测和控制。通过对进程和 IP 地址作智能流量控制,对不同进程的带宽做检测和控制。按用户角色、应用进程和时间等多个方面,对进程带宽做控制,也可以针对 IP 地址作网络流量管理。对需要分析的 IP 协议分成 TCP、UCP 和 ICMP 等作不同处理[12]。TCP 头有序列号和确认号等,包内标志位有 URG、ACK、PSH、RST、SYN 和 FIN 等。对 TCP 连接而言,每个连接都保存在状态链表,建立基于状态图的协议分析模型,在针对 TCP 协议的安全攻击可对状态作匹配并拦截报警。SYN COOKIE/SYN PROXY 防护是对 SYN 包源地址作探测,以地址真实存在与否决定是否建立 TCP 连接。ACK Flood 会影响一些 Web 服务器。UDP Flood 属于流量型 DOS 攻击。对 UDP 攻击可判断参数:数据包大小,对特定端口攻击的拦截。ICMP 攻击可采用对 ICMP 报文筛选方法。HTTP GET 类型攻击可对 Get 请求/每秒作统计,如超出阈值则对相应的 URL 等作报警或拦截。UDP DNS Query Flood 攻击,查询 DNS 域名会使服务器超载。对 DNS 基于进程的流量做检测和限制。

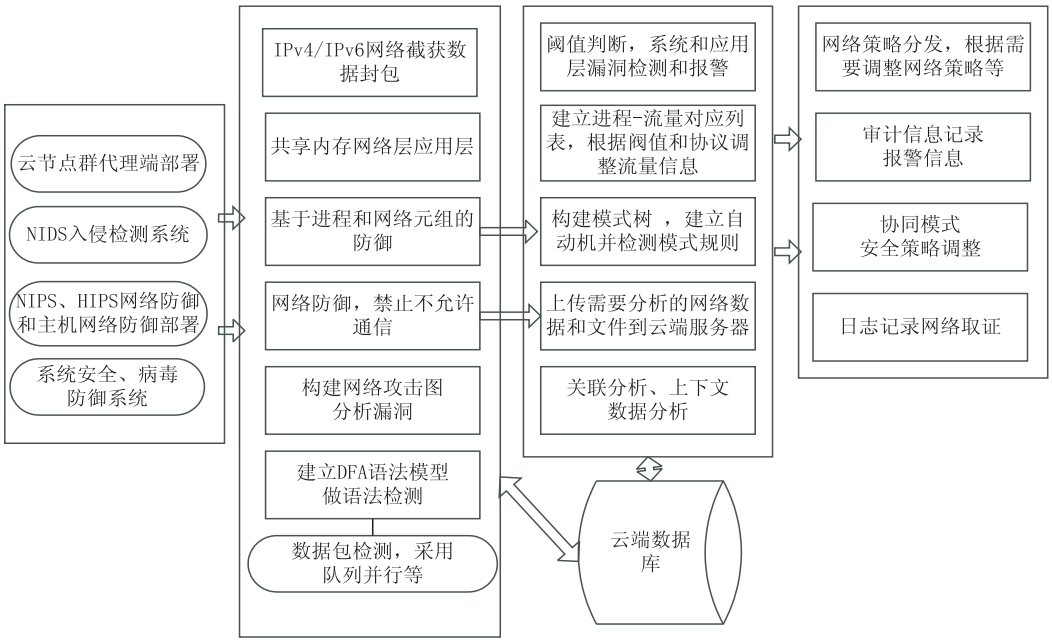

图 6　网络防御整体功能图

系统采集需要的网络数据在应用层或分布式系统做统一的网络大数据智能检测。IDS 对特征作单独匹配,不能检测多个事件的关联攻击。云网络需要对多个安全功能部件协同计算。在云分布式节点部署 Agent客户端,采集需要的网络和文件数据,上传到云端分析或做并行数据分析,接收下发的防御策略和指令。根据网络安全总体态势部署相应的网络防御策略。协同就是不同防御功能、策略、报警和数据分析等动态的部署。可以采用 P2P 等通信模式做代理与云端的通信,下发策略和指令等。利用并行算法(如 MapReduce 等)对文件数据作快速分析和检测。如 NIDS 与网络层防火墙协同,可以截断网络攻击。NIDS 可及时发现被攻陷的网络主机并报警[13]。

构建可信网络主要包括对访问用户做权限认证、网络数据通信安全、检测管理、网络取证、审计和云端检测等方法。网络协同方法可以参考选择各类并行计算,如云计算网和 P2P 网络等。考虑到性能瓶颈和下一代网络的兼容性,在网络栈的多个层次对不同的威胁做防范,采用分布式数据库协同通信模式更加安全,利用网络安全态势等分析,构建智能网络防御系统。自动更改规则、部署策略、采集各类数据等。确保在并行和规模网络计算时的网络取证和安全防御。

5　结束语

在复杂云网络环境下,对网络通信做检测和控制对安全至关重要。网络安全系统直接影响网络吞吐量和系统安全。基于 P2P 的僵尸网络难以截断和防御,文中从网络协同部署 NIDS 和 HIPS 的方法,在云分布式节点和云端等部署系统,并提出了基于最大不重复字符串的改进 Sunday 算法。算法在避免重复比较方面有自己的特色。云计算网络安全系统的协同工作十

(下转第 99 页)

研究与发展,2008,45(3):400-407.
[3] 黄　政,王　新. 网络编码中的优化问题的研究[J]. 软件学报,2009,20(5):1349-1361.
[4] 俞立峰,杨　琼,于　娟,等. 防窃听攻击的安全网络编码[J]. 计算机应用研究,2012,29(3):813-818.
[5] Cai Ning,Chan T. Theory of secure network coding[J]. IEEE Journals & Magazines,2011,57:416-423.
[6] 周业军,李　晖,马建峰. 一种防窃听的随机网络编码[J]. 西安电子科技大学学报:自然科学版,2009,36(4):696-701.
[7] 曹张华,唐元生. 安全网络编码综述[J]. 计算机应用,2010,30(2):499-505.
[8] 张盛勇,陈世康. 网络编码的安全问题初探[J]. 通信技术,2012,45(1):105-107.
[9] Ho T,Leong B,Koetter R,et al. Byzantine modification detection in multicast networks using randomized network coding[C]//Proc of IEEE international symposium of information theory. [s. l.]:IEEE,2004.
[10] Jaggi S,Langberg M,Katti S,et al. Resilient network coding in the presence of byzantine adversaries[C]//Proc of international conference on computer communications. [s. l.]:[s. n.],2007.
[11] Yu Z,Wei Y,Ramkumar B,et al. An efficient signature-based scheme for securing network coding against pollution attacks[C]//Proc of international conference on computer communications. [s. l.]:[s. n.],2008.
[12] Agrawal S,Boneh D. Homomorphic MACs:MAC-based integrity for network coding[C]//Proc of international conference on applied cryptography and network security. [s. l.]:[s. n.],2009.
[13] Zhao F,Kalker T,Medard M,et al. Signatures for content distribution with network coding[C]//Proc of IEEE international symposium on information theory. [s. l.]:IEEE,2007.
[14] He Ming,Chen Lin,Wang Hong,et al. Adapkeys:an adaptive security scheme for network coding[C]//Proc of IEEE Asia-Pacific services computing conference. Guilin:IEEE,2012:309-314.
[15] Kehdl E,Li B. Null keys:limiting malicious attacks via null space properties of network coding[C]//Proc of international conference on computer communications. [s. l.]:[s. n.],2009.
[16] Zhang Peng,Jiang Yixin,Lin Chuang,et al. Padding for orthogonality:efficient subspace authentication for network coding[C]//Proc of international conference on computer communications. Shanghai:IEEE,2011:1026-1034.
[17] 刘济恺. 防污染的安全网络编码研究[D]. 成都:西南交通大学,2014.
[18] Canetti R,Garay J,Itkis G,et al. Multicast security:a taxonomy and some efficient constructions[C]//Proc of international conference on computer communications. [s. l.]:[s. n.],1999.
[19] Gkantsidis C,Rodriguez P. Cooperative security for network coding file distribution[C]//Proc of international conference on computer communications. [s. l.]:[s. n.],2006.

(上接第 93 页)

分重要,动态截断可疑网络数据流。根据安全态势做智能化网络防御。基于进程和网络元组的网络流量和连接控制,基于并行算法的协同安全组件,研究了提高云计算网络的安全机制的各种方法。

参考文献:

[1] 姜　伟,方滨兴,田志宏,等. 基于攻防博弈模型的网络安全测评和最优主动防御[J]. 计算机学报,2009,32(4):817-827.
[2] 胡　平,李　臻,彭纪奎. 基于入侵检测的分布式防火墙的应用研究[J]. 微电子学与计算机,2011,28(6):126-130.
[3] Russinovich M,Solomon D A. Windows internals:including Windows server 2008 and Windows Vista[M]. [s. l.]:Microsoft Press,2009.
[4] 马兆丰,顾　明,孙家广. 基于角色的可信数字版权安全许可授权模型[J]. 清华大学学报:自然科学版,2006,46(4):534-538.
[5] 吴　涛,张毛迪,陈传波. 一种改进的统计与后串最大匹配的中文分词算法研究[J]. 计算机工程与科学,2008,30(8):79-82.
[6] 李鸿彬,林　浒,侯辉超,等. 一种 SIP 分布式洪泛攻击的减弱方法[J]. 小型微型计算机系统,2012,33(5):995-999.
[7] 胡建理,周　斌,吴泉源,等. P2P 网络环境下基于信誉的分布式抗攻击信任管理模型[J]. 计算机研究与发展,2011,48(12):2235-2241.
[8] 陈伟东,王　超,张　力,等. 服务器系统安全内核研究与实现[J]. 计算机应用与软件,2013,30(3):304-307.
[9] 陈伟东. 一种 HTTP 通信内容检测的方法:中国,CN104022924A[P]. 2014-09-03.
[10] Ficara D,Giordano S,Procissi G,et al. An improved DFA for fast regular expression matching[J]. ACM SIGCOMM Computer Communication Review,2008,38(5):29-40.
[11] 亓亚烜,李　军. 高性能网包分类理论与算法综述[J]. 计算机学报,2013,36(2):408-421.
[12] 陈伟东,张　力. Windows Rootkit 分析与检测综合方法[J]. 信息化纵横,2009(12):10-15.
[13] Modi C,Patel D,Borisaniya B,et al. A survey of intrusion detection techniques in cloud[J]. Journal of Network and Computer Applications,2013,36(1):42-57.