文章编号:1671-4598(2018)07-0038-03 DOI:10.16526/j.cnki.11—4762/tp.2018.07.008 中图分类号:TP393.08 文献标识码:A

低敏感路由协议攻击自适应监测系统设计

罗肖辉[1],郭 雅[2]
(1.广州商学院 实验实训中心,广州 511363;
2.广东创新科技职业学院 信息工程学院,广东 东莞 523960)

摘要:路由协议是由不同层次的多个协议组成的,当前的路由协议攻击监测系统无法从路由协议层次间的数据链路层中获取大量的数据包,使系统无法在短时间内实现数据的采集和传输,存在带宽占有率低、响应时间长、误比特率高的问题;提出一种路由协议攻击监测系统构架,对路由协议进行解析,在不影响监测效率的情况下及时控制数据采集频率,减少系统的带宽占有率;对网络数据采集过滤器和分接头的联系以及信号中错误比特数的处理做了较为详细的阐述,设计了信息发布方式,并对数据包规则进行描述;实验结果表明,该系统的响应时间短、带宽占有率低、误比特率低。

关键词:低敏感;路由协议;监测系统

Design of Adaptive Monitoring System for Low Sensitive Routing Protocol Attack

Luo Xiaohui[1], Guo Ya[2]
(1. Department of Educational Information Technology, Guangzhou College of Commerce, Guangzhou 511363, China;
2. School of Information Engineering, Guangdong Innovative Technical College, Dongguan 523960, China)

Abstract: The routing protocol is composed of multiple protocols at different levels. The current routing protocol attack monitoring system can not obtain a large number of data packets from the data link layer between the routing protocol layers, so that the system can not realize the data acquisition in a short time and transmission, there is a low bandwidth occupancy, long response time, high bit error rate. This paper proposes a routing protocol attack monitoring system architecture, which analyzes the routing protocol and controls the data acquisition frequency without affecting the efficiency of monitoring. The bandwidth occupancy of the system is reduced. The connection between the network data acquisition filter and the tap and the signal processing of the number of errors in the bit to do a more detailed description. The design of the information release, and the rules of the packet are described. The experimental results show that the system has short response time, low bandwidth occupancy rate and low bit error rate.

Keywords: low sensitivity; routing protocol; monitoring system

0 引言

随着计算机技术和互联网技术的快速发展,云计算、物联网、电子商务和三网融合的技术得到广泛的普及[1]。人们对网络的依赖越来越严重,对网络技术的依赖推动了网络技术发展的同时,也给信息的安全带来了隐患,尤其是给路由协议网络基础设施的安全带来了严峻的考验[2]。

当前路由协议和网络基础设施在设计时只考虑到了网络通信的便利,并没有考虑网络的安全问题[3]。导致目前的网络安全形式较为严峻,因此也出现了海量针对网络协议尤其是路由协议的攻击方式[4]。大量网络安全事件的发生和网络空间问题的不断扩大,使网络安全问题逐渐被网络安全研究人员和各国政府所关注[5]。目前被广泛使用的路由协议不能对企业通信和 OSPF 通信进行加密和认证,对新型的攻击方式存在诸多的防范漏洞,使系统中存在较多的错误信号[6]。为解决上述问题,提出了一种低敏感路由协议攻击自适应监测系统设计方法,该方法对新型的攻击方式进行研究,可以在最短的时间内了解其攻击方式,给出有效的防范措施来保障网络信息的安全,该方法的提出得到了广泛的关注。

路由协议攻击监测系统保障了网络用户的信息安全[7]。为了使路由协议攻击监测系统可以更好的应用到网络安全中,需要对路由协议攻击监测系统进行深入的研究和分析[8]。基于虚拟器技术的路由协议攻击监测系统以 PXIe—5196 数字化仪器为主要硬件,采用虚拟仪器技术对网络信号进行监测和识别,该方法具有信号采集和数据存储的功能,通过数字滤波和触发限制对网络信号进行处理,该方法可以有效的降低系统存储数据的压力,但系统的数据传输速度较慢、响应时间较长[9]。基于链路覆盖的路由协议攻击监测系统对网络中所有的节点都进行监测,网络节点根据自身的内存阈值加载路由协议监测系统的功能模块,

收稿日期:2017-09-04; **修回日期**:2017-11-29。

作者简介:罗肖辉(1980-),男,广东信宜人,实验师,主要从事网络安全技术应用 虚拟云平台方向的研究。

并采用优化协调机制对网络节点进行优化，每条通信链路上都由多个网络节点进行覆盖和监测，该方法监测的可靠性较高，但系统的带宽占有率高和误比特率高[10]。

1　路由协议解析

对路由协议进行解析，是完成低敏感路由协议攻击自适应监测系统的基础。路由协议是由不同层次的多个协议组成的，低敏感路由协议攻击自适应监测系统中上层协议的各种工作需要通过下层协议来完成并实现，低敏感路由协议攻击自适应监测系统的路由协议层次结构图如图 1 所示。

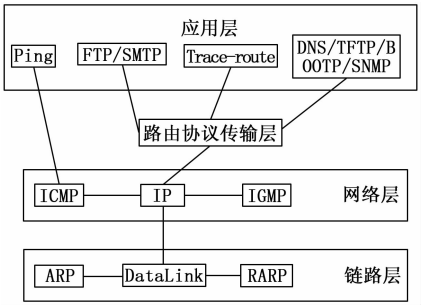

图 1　路由协议攻击监测系统的路由协议层次结构图

从低敏感路由协议攻击自适应监测系统的路由协议层次分类上看，下层协议是上层协议数据包的大类，要先确保下层协议数据包的特征满足之后才能考虑到上层协议数据包的特征。在低敏感路由协议攻击自适应监测系统中下层协议可以体现上层协议事项的一些细节，如可以通过 IP 首部的协议字段确定协议是 UDP 协议还是 TCP 协议。协议解析可以将数据链路层中获取的数据包通过协议层次的结构解析后传送到 Packet 结构中并储存，在解析数据包时可以检查数据包的合法性。低敏感路由协议攻击自适应监测系统设计协议解析的流程图如图 2 所示。

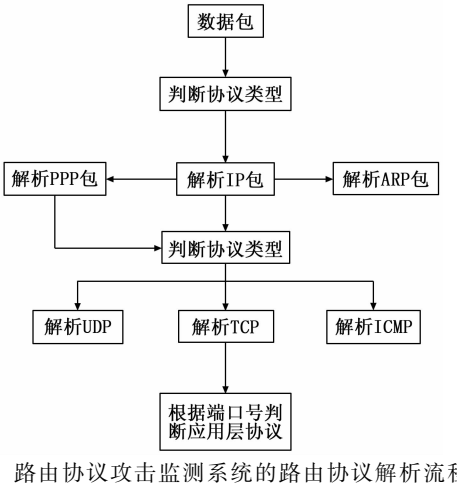

图 2　路由协议攻击监测系统的路由协议解析流程图

路由协议解析体现了协议分析的基本思想，进行规则匹配时，先进行协议层首部的匹配，若匹配成功，进行数据匹配，进行数据匹配时，可以跳过低敏感路由协议攻击自适应监测系统协议层首部的匹配，提高了低敏感路由协议攻击自适应监测系统的监测效率。

2　监测系统的构建

2.1　带宽占有率的降低

低敏感路由协议攻击自适应监测系统在采集数据时会占用一定的带宽，系统通过审计数据采集功能可以对数据采集的频率进行控制，减少系统的带宽占有率。系统的审计数据采集由数据接收、数据请求、数据储存和代理库构成，图 3 为监测系统的带宽监测界面。

1）监测系统通过数据接收和请求方式完成了数据在系统中的需求，系统的数据请求主要是向代理库中传输数据，并通过数据接收功能接收代理库中的数据。

2）采用数据储存功能将数据存入低敏感路由协议攻击自适应监测系统的数据库中。

3）代理库的主要功能是记录用户登录监测系统的时间、退出监测系统的时间和登录主机的 IP 地址。

图 3　监测系统的带宽监测界面

2.2　误比特率的降低

网络数据采集是截获网络协议模型中各个协议层次数据包的主要途径，在截获网络数据包时，需要将低敏感路由协议攻击自适应监测系统的网卡调设为混合工作的模式，网络数据采集是低敏感路由协议攻击自适应监测系统中监测引擎数据的来源。低敏感路由协议攻击自适应监测系统完成网络数据的截获分为两部分，分别是网络数据包过滤器和网络分接头。

1）网络分接头从低敏感路由协议攻击自适应监测系统的驱动设备中采集网络数据包拷贝，将数据包拷贝传输给低敏感路由协议攻击自适应监测系统的监听设备。

2）过滤器决定了网络数据包的接收方式和拒绝方式，并将数据包中的一部分数据进行拷贝传送到应用程序中。

当网络数据包到达低敏感路由协议攻击自适应监测系统的网络接口设备时，一般采用链路层设备的驱动器将数据包传送到系统协议进行处理，低敏感路由协议攻击自适应监测系统驱动器会调用网络接口监听中的数据包，并将数据包传送到每个监控设备的过滤器中，过滤器对数据包是否被接收并保存进行判断。

1）若网络数据包锁定的目标地址不是本机地址，则终止驱动程序并返回，

2）若数据包锁定的目标地址为本机地址，则继续运行路由协议的处理过程。

网络数据采集通过网络数据包过滤器和网络分接头决

定了网络数据包接收和拒绝的方式，并将采集到的数据包拷贝传送到系统的监听设备，减少了系统信息中存在的错误比特数，降低了系统的误比特率。误比特率显示界面如图 4 所示。

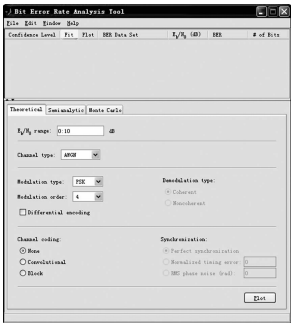

图 4 误比特率显示界面

2.3 页面刷新响应时间的减少

低敏感路由协议攻击自适应监测系统通过报警响应功能对系统所产生的警报信息进行排序和转发。当低敏感路由协议攻击自适应监测系统中出现特殊情况和异常时，系统通过报警响应功能发出警报信号，系统包含多个目的地址，在发送报警信号时使用，可以快速的将警报信息传送到用户客户端，确保用户可以及时的看到报警信息，减少系统页面刷新的响应时间。

攻击模式数据库中含有三种动作，分别是 Alert、Pass 和 Log，警报响应只对 Alert 事件的触发发送警报信号，警报信号发送的地址是可以配置的。系统用户可以自己创建目的地址，并采用第三方程序传真和电子邮件的方式发送警报信息，每个警报信息可以传送到多个目的地址。

2.4 数据包的规则描述

低敏感路由协议攻击自适应监测系统的攻击模式库对网络数据包进行规则描述时具有以下几个要求。首先，要在单独的一行内完成对数据包的规则描述。其次，网络数据包的规则描述分为两个部分，分别是规则选项和规则头。其中规则头包含了目的地址、规则动作、IP 源地址、协议、源端口、目标端口值和子网掩码等。规则选项包含了需要检查的数据包区域位置信息和警报信息。

2.5 信息发布方式

经过低敏感路由协议攻击自适应监测系统监测引擎的数据都被保存在系统的数据库中，系统用户可以通过信息备份和数据库维护对信息进行查询，信息备份是基于 web 方式，数据库维护方式是通过进入监测系统的管理平台。

3 实验方法及步骤

本次测试在 Solr 平台完成，低敏感路由协议攻击自适应监测系统在获取网络中的数据信息时，会对网络资源造成一定的消耗，使路由协议攻击监测系统的监测结果受到一定的影响，若路由协议攻击监测系统采集数据的频率过低，得到的参数结果与实际结果相差较大。若路由协议攻击监测系统采集数据的频率过高，会使带宽的消耗增加，对路由协议攻击监测系统的路由器性能造成影响。因为低敏感路由协议攻击自适应监测系统在采集数据时会占用一定的带宽，因此用系统带宽的占有率来判断对正常端口流量的影响，表 1 为低敏感路由协议攻击自适应监测系统的带宽占有率测试结果。带宽占有率的计算公式如下：

$$\text{带宽占有率} = \text{管理所占的节数} / \text{所有字节数} \quad (1)$$

表 1 低敏感路由协议攻击监测系统带宽占有率

实验序号	管理所占字节数/字节	所有字节数/字节	带宽占有率(%)
1	130	22272	0.580
2	135	22385	0.600
3	140	23000	0.608
4	150	23121	0.648
平均	138	22694	0.609

分析表 1 可知，在低敏感路由协议攻击自适应监测系统测试中管理所占字节数平均为 138 字节，所有字节数平均为 22694 字节，带宽的平均占有率为 0.609%。监测结果对系统的影响很小，可以忽略不计，低敏感路由协议攻击自适应监测系统较为稳定。

为了检验低敏感路由协议攻击自适应监测系统的性能，需要对低敏感路由协议攻击自适应监测系统进行性能测试，创建一千五百万条攻击事件，包括路由协议攻击事件、网站攻击事件和终端攻击事件，监测低敏感路由协议攻击自适应监测系统页面刷新的响应时间和监控响应时间 CPU 的使用率，测试结果如表 2 所示。

表 2 低敏感路由协议攻击监测系统性能测试结果

事件数/万条	响应时间/s	CPU(%)
50	<3	<70
100	<3	<70
500	<3	<70
1000	<3	<70
1500	<3	<70

分析表 2 可知，无论攻击事件数为五十万条、一百万条、五百万条、一千万条、一千五百万条低敏感路由协议攻击自适应监测系统的页面刷新响应时间都小于 3 秒，响应时间 CPU 在 70%以下，说明低敏感路由协议攻击自适应监测系统在受到路由协议攻击、网站攻击和终端攻击事件时，系统页面刷新的速度不受到影响，能够快速的加载出页面，系统响应时间 CPU 的使用率不因受到事件攻击而升高，低敏感路由协议攻击自适应监测系统的可用性较高。

误比特率指的是在数据通信中，在一段时间内系统收到的数字信号中含有错误的比特数与这段时间内收到的总数字信号数的比，误比特率越低系统的精确性越高。采用本文方法和文献［9］方法、文献［10］方法进行测试。

分析图 5 可知本文方法的误比特率为 0.17%，本文方法通过数据采集中的网络数据包过滤器和网络分接头决定

（下转第 56 页）