路由器拟态防御能力测试与分析

马海龙, 江逸茗, 白 冰, 张建辉
解放军信息工程大学信息技术研究所 郑州 中国 450000

摘要 路由器是网络中的核心基础设备, 但其面对基于漏洞和后门的攻击时却缺少有效的防御手段。拟态防御机制作为一种创新的主动防御方法引入到路由器的设计架构中, 构建了路由器拟态防御原理验证系统。结合拟态防御机制的特性和路由器的特点, 提出了针对路由器拟态防御原理验证系统的测试方法, 并按照测试方法对该系统进行了全面测试, 包括基础性能测试, 拟态防御机制测试以及防御效果测试。测试结果表明, 路由器拟态防御原理验证系统能在不影响路由器基本功能和性能指标的前提下实现了拟态防御机制, 拟态防御机制能够改变固有漏洞或者后门的呈现性质, 扰乱漏洞或后门的可锁定性与攻击链路通达性, 大幅增加系统视在漏洞或后门的可利用难度。

关键词 路由器; 拟态防御; 测试方法; 漏洞; 后门
中图法分类号 TP 393 DOI 号 10.19363/j.cnki.cn10-1380/tn.2017.01.004

Tests and Analyses for Mimic Defense Ability of Routers

MA Hailong, JIANG Yiming, BAI Bing, ZHANG Jianhui
Institute of Information Technology, PLA Information Engineering University, Zhengzhou 450000, China

Abstract Routers are core devices in networks, but are still in lack of effective defense method against vulnerability-based and backdoor-based attacks. Therefore, the mimic defense mechanism, which is an implementation of innovative active defense theory, is employed into the architecture design of routers. Based on this mechanism, a "Verification System for the Mimic Defense Theory of Routers" is designed. With the characteristic of mimic defense mechanism and routers, a test method to evaluate the "Verification System for the Mimic Defense Theory of Routers" is proposed and implemented which include basic performance test, mimic defense mechanism test and defense effect test. Test results show that with no influence on basic performance, the "Verification System for the Mimic Defense Theory of Routers" could implement the mimic defense mechanism. What's more, it could also change the presentation of backdoor and vulnerability, disturb the locking process of backdoor or vulnerability attack and the accessibility of attack link, and significantly increase the difficulty of backdoor or vulnerability exploitation.

Key words router; mimic defense; test method; vulnerability; backdoor

1 背景

路由器位于网络空间底层, 互联多种异构网络, 负责网络中数据传递路径的计算和查表转发工作, 是网络空间中最为重要的核心基础设备之一。因此, 路由器的安全对于网络本身的安全乃至整个国家的信息安全都具有极其重要的意义。从另一方面来说, 由于设计上的疏漏或是一些人为的刻意安排, 导致路由器自身不可避免地存在一些漏洞或后门。据斯诺登披露, 美国国安局专门研制了针对部分品牌路由器的攻击工具[1]; 国家互联网应急中心对 Cisco、Linksys、Netgear、Tenda、D-link 等主流网络设备厂商的多款路由器产品进行分析, 确认其部分型号的路由器存在预置后门漏洞[2]。正是由于路由器在网络中的核心地位, 使其一旦被攻击者控制, 将使网络上传递的私密数据面临被窃取的危险, 攻击者甚至可以借助被攻击的路由器传播虚假信息、篡改数据流向、瘫痪整个网络等。如果说主机的安全威胁仅影响到主机自身, 那么路由器的安全威胁将影响到与路由器相连接的整个网络。

由于路由器在设计实现上的封闭特性, 入侵检测、杀毒软件等安全防护措施无法部署在路由器内部。而且由于路由器系统的代码量巨大, 缺乏高效的漏洞上报和动态修复机制, 导致路由器自身存在大

通讯作者: 马海龙, 博士, 副研究员, Email:longmanclear@163. com。
本课题得到国家自然科学基金创新研究群体项目(No.61521003)和国家重点研发计划(2016YFB0800100, 2016YFB0800103)资助。
收稿日期: 2016-09-20; 修改日期: 2016-11-03; 定稿日期: 2016-12-02

量潜在的漏洞。这些因素都导致了路由器的安全等级不高, 在面临具有国家背景的有组织攻击时, 一些核心路由器将很快沦陷。因此, 有必要开拓新的防御思路来提高路由器的防御能力。

为破解网络防御困局, 一些网络技术发达国家积极转变防御理念, 提出了“主动防御”的概念, 以防范未知漏洞或威胁[3,4]。“主动防御”是一种前摄性防御, 通过采用一些不依赖于特定攻击特征的防御措施, 使攻击者无法完成对目标的攻击, 或者使系统在无需人为被动响应的情况下预防未知攻击。以美国为首的一些国家已经提出了一些主动防御的实现思路: 1)“数字源”(验证)技术确保根源数据可信; 2)利用“移动目标防御技术”[5]确保攻击只能一次生效; 3)利用“可信启动硬件”技术确保硬件在启动时能够发出实时报告; 4)通过“激发本能”网络健康防御技术确保诊断实时进行[6]。

最近几年国内也涌现出了一些解决网络安全问题的主动防御新思路, 其中邬江兴院士提出了一种拟态防御思想, 期望通过“改变游戏规则”的技术创新, 彻底扭转网络空间攻防能力严重失衡的格局。目前已形成了完整了拟态防御理论体系, 其技术愿景是: ①在给定条件下系统能同时应对已知和未知网络安全威胁; ②允许基于“有毒带菌”软硬构件搭建系统; ③具有不依赖传统安全手段的内生安全增益; ④探索基于系统架构技术突破自主可控发展瓶颈之新途径[7,8]。

基于拟态防御思想, 研制完成了“路由器拟态防御原理验证系统”(简称“拟态路由器”), 该系统是国内第一台具备主动防御能力的路由器。该系统通过异构执行体的相异性设计、动态调度技术、冗余部件、多模裁决技术等, 提高路由器的安全防护能力, 使路由器能够抵御基于未知漏洞和后门的网络攻击。

为了评估“路由器拟态防御原理验证系统”抵御网络攻击的能力, 验证拟态防御机制有效性, 需要对该系统进行全方位的测试。但由于被测对象采用了全新的安全防御理念, 因此除了对路由器的基础性能进行测试以外, 还需要对被测系统中拟态防御机制的运行实现情况, 以及系统对漏洞攻击和后门攻击的防御效果进行测试。本文通过对大量自测数据和第三方测试数据的解读, 深入分析和评估了拟态路由器的安全防护能力。

文章第二节对拟态路由器的架构和原理进行了概述, 第三节介绍了整体测试思路, 第四节介绍了路由器基础性能测试方法和分析结果, 第五节阐述了拟态防御机制的测试方法和分析结果, 第六节阐述了拟态防御效果的测试方法及分析结果, 第七节对全文进行了总结。

2 拟态路由器概述

拟态防御思想是: 分离元功能与具体实现结构的耦合关系, 构建多个功能等价、异构冗余的多执行体环境, 通过动态调度机制建立元功能和执行体的实际映射关系, 在保证系统功能不变的条件下, 充分利用动态性、多样性、随机性来隐藏执行体内部存在的各种“暗功能”, 使得攻击者难以建立起持续可靠的攻击链。进一步引入多模裁决机制, 对多执行体的输出结果进行多模裁决输出, 确保输出结果的正确性。

拟态路由器是拟态防御思想在路由器领域的具体实践, 其实现架构如图 1 所示。

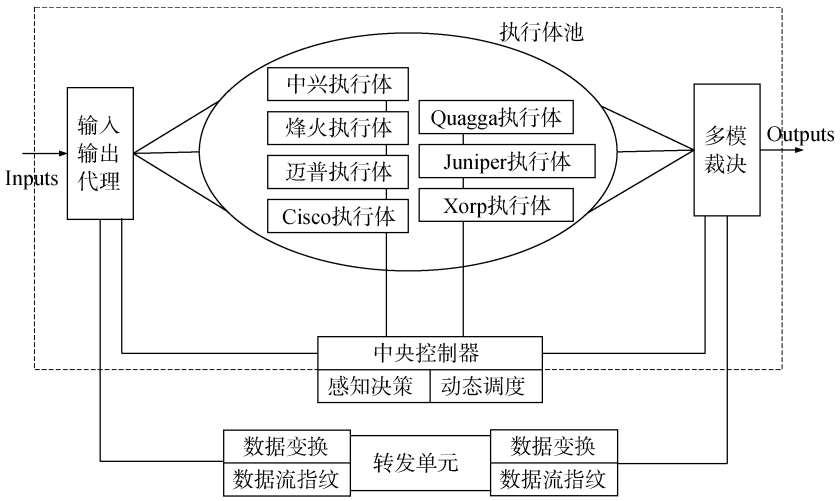

图 1 拟态路由器架构

系统包括输入输出代理、中央控制器、转发单元、多模裁决以及执行体池。其中, 中央控制器包括感知决策和动态调度模块; 转发单元包括数据变换和数据流指纹模块; 执行体池包括七个功能等价的异构执行体, 受中央控制器调度上线和下线, 在线执行体的角色可以分为 worker 和 inspector 两种, worker 执行体负责整个路由器的对外呈现, 因此在任意时刻有且只有一个, inspector 执行体负责为多模裁决提供支撑, 其数量由系统预先配置和执行体池大小决定, 可以有多个, 一般为偶数个。

拟态路由器的工作原理如下:

(1) 输入输出代理对接收到的外部数据进行识别分流和复制分发, 将数据平面的数据送至转发单元进行处理, 将控制/管理平面的数据发送至在线执行体(worker 和 inspectors)进行处理。

(2) 在线执行体(worker 和 inspectors)对收到的控制/管理平面的数据进行独立处理, 并将结果发送给多模裁决。

(3) 多模裁决对收到的在线执行体的数据进行裁决, 按照系统预设策略选取输出, 并将比对结果发送至中央控制器。

(4) 中央控制器收到多模裁决上报的裁决结果, 处理出现异常的执行体。

如果只有 inspector 出现异常, 从执行体池中按照既定策略选取等量的执行体替代异常执行体工作, 并将异常执行体下线清洗。如果执行体池中剩余执行体数量不足, 则将它们全部选取上线, 并修改相应的运行状态参数(在线执行体数量)。

如果 worker 出现异常, 则从当前 inspector 中选取一个工作正常的执行体转换角色为 worker, 当前出现问题的 worker 执行体转换角色为 inspector, 然后处理过程和只有 inspector 出现异常的情况相同。

(5) 中央控制器执行切换调度策略, 即使在未发现异常的情况下, 也会根据设定的参数, 进行如下操作:

切换上线执行体的角色, 即 worker 和 inspector 的角色转换。

调度新的执行体上线替代当前执行体工作。

(6)数据平面的数据在进出转发单元时会经过数据变换和数据指纹模块进行处理, 防止攻击者利用数据平面数据的后门/漏洞, 导致路由工作异常或者瘫痪。

3 拟态路由器测试方法设计

对传统路由器的测试至少包括功能测试和性能测试, 此外还有稳定性测试、可靠性测试、一致性测试和互操作性测试等。其中, 功能测试主要用于评估路由器的接口功能、通信协议功能、数据包转发功能、路由信息维护功能、管理控制功能、安全功能。性能测试主要考查路由器的吞吐量、时延、丢包率、背靠背帧数、系统恢复时间等性能指标[9]。

针对传统路由器的测试方法虽然能对路由器的功能、性能、可靠性等指标做出评判, 但在评估路由器抵御网络攻击能力方面仍然没有较好的解决方法, 而且传统的测试方法也无法对拟态防御机制在路由器中的实施过程进行验证。因此, 本文设计了针对拟态防御机制的测试方法以及对防御效果的测试方法, 这两种方法综合利用开放内部模块接口、结果对照分析等手段, 分别从实现过程和实现效果两个角度对被测对象的防御能力进行评估。按照新的测试思路, 可将测试内容分为以下三个部分:

(1) 路由器基础性能测试

主要目的是检测拟态路由器在其架构中加入了用于实现拟态防御机制的相关单元和模块后, 是否会对系统的转发性能和路由计算等基础能力产生影响。

(2) 拟态防御机制测试

主要目的是测试实现拟态防御机制的相关模块是否能够按照设计要求正常运行, 并能有效地实现拟态防御机制。

(3) 防御效果测试

主要目的是测试在不消除路由器固有漏洞或后门的前提下, 被测系统是否能够:

改变固有漏洞或者后门的呈现性质。

扰乱漏洞或后门的可锁定性与攻击链路通达性。

大幅增加系统视在漏洞或后门的可利用难度。

测试的整体构架如图 2 所示。

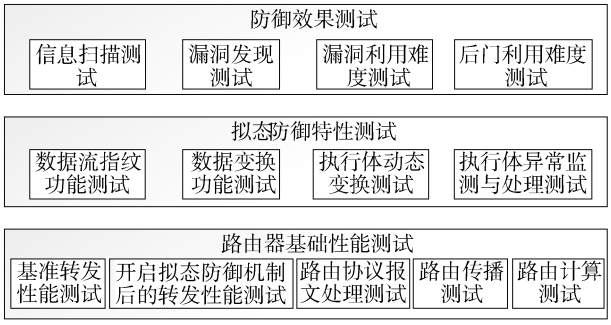

图 2 测试架构设计

测试方法可以分为两类: 符合型测试和开放配合型测试[10]。对于有标准或设计规范可遵循的内容, 按照符合型测试方法, 测试被测对象与相关标

准、理论框架、设计要求等的一致性[11]。而对于网络攻击，攻击链前一环节的成功是后续环节开展的前提，为突破这一限制，覆盖攻击链的所有环节，评估拟态机制对斩断攻击链各个环节的效果，采用开放配合型测试方法。其具体方法为：公开系统实现结构，设置内部观测点、植入后门、关闭拟态机制等。

测试环境设置如图 3 所示，被测系统的一个接口与互联网进行连接，接收来自外部网络的攻击，另外 3 个接口与思博伦测试仪构建的虚拟网络相连，虚拟网络中虚拟了视频服务器、邮件服务器、终端等业务节点，也包括了用于实施攻击的虚拟节点。第四、五、六节均在此拓扑环境下进行测试与分析。测试工具包括思博伦测试仪 TestCenter、Wireshark[12]、Nmap[13]、Nessus[14]、Metasploit[15]等。

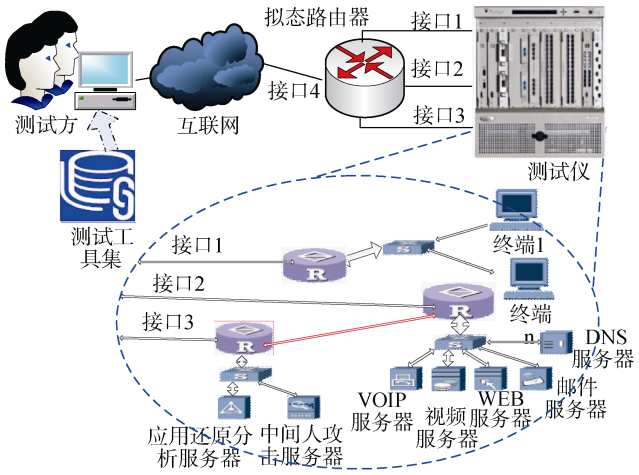

图 3 测试拓扑环境

4 路由器基础功能与性能测试

本节测试的目的是为了验证在路由器中引入拟态防御机制后，系统的基础性能是否得到保证，这是进行安全性测试的前提。

基础性能测试包括路由协议功能测试和转发性能测试两部分内容。测试采用思博伦测试仪 TestCenter 完成协议功能测试和性能测试。

4.1 路由协议功能测试

该测试的目的是验证系统实现的路由协议功能是否符合标准协议规范。测试的对象设为 Open Short Path First(OSPF)协议[16]。测试方法是，通过思博伦测试仪向被测系统发送特定数据包，依据 OSPF 协议标准进行符合性测试。测试结果如表 1 所示。

从测试结果可以看出，拟态路由器所实现的 OSPF 协议符合 RFC 标准，可以认为拟态防御机制的引入不影响路由器原有的路由协议功能。

表 1 OSPF 协议功能测试结果

测试编号	测试项	测试结果
1	OSPF 报文头合法性检查	通过
2	HELLO 报文头合法性检查	通过
3	各种接口发送的 HELLO 报文	通过
4	接收 HELLO 报文	通过
5	数据库同步过程中的主/从关系的确定	通过
6	发送和接收数据库描述报文	通过
7	接收非法数据库描述报文	通过
8	对各种链路状态广告的数据库同步	通过
9	发送和接收链路状态请求报文以及链路状态更新报文和链路状态确认报文	通过
10	链路状态更新报文合法性检查	通过
11	路由传播	通过
12	最短路径优先算法	通过

4.2 转发性能对比测试

该测试的目的是对比系统在引入拟态防御机制前后转发性能的变化，从而比较拟态防御机制对于路由器基础转发性能的影响。

测试方法是，第一步，关闭系统的拟态防御功能(此时系统等价为一台传统路由器)，测试系统的转发性能，作为性能对比的基准；第二步，分别测试在单独开启系统的数据变换或动态调度功能的条件下，系统的转发性能；第三步，在同时开启数据变换和动态调度功能(即开启系统的全部拟态功能)的条件下，测试系统的转发性能。

采用测试仪的 GE 接口与被测系统对接，在 1000Mbps 速率下测试系统的转发性能指标。在丢包率和时延抖动均为 0 的条件下，选取系统的吞吐率和时延作为转发性能的评价指标。每一步测试的帧大小包括 64, 128, 256, 512, 1024, 1280 和 1518 字节。测试结果如表 2 所示。

表 2 转发性能对比测试结果

测试条件	平均吞吐率(%)	平均时延(ms)
基准(关闭拟态功能)	85.7	0.35
仅开启数据变换	83.7	0.35
仅开启动态调度	84.2	0.38
开启数据变换和动态调度	85.4	0.39

从测试结果来看，拟态路由器在部分或者全部开启拟态防御功能的情况下，其转发性能(吞吐率和时延)与基准转发性能相比，并无明显下降，因此可以认为，拟态防御机制的引入对路由器的基本转发性能并无明显影响。

综上所述, 拟态路由器在引入拟态防御机制后, 仍然能够保证其作为路由器的基本功能, 且性能指标无明显下降。

5 拟态防御机制测试及结果分析

为了实现拟态防御的目标, 拟态路由器在其体系架构中加入了数据变换机制、数据流指纹生成机制、执行体动态调度机制、多模裁决机制等。而要评测拟态防御机制的防御效果之前, 首要测试拟态路由器是否实现了声称的拟态防御机制, 确定这些机制能够按照设计要求完成其预定的功能。

在数据层面, 针对数据变换机制、数据流指纹生成机制的两项测试, 需要构造相应的测试数据包, 并在系统外部和内部设立多个流量监测点, 通过对不同观测点上的数据进行对比, 判断相应的功能是否被实现。数据变换机制、数据流指纹生成机制的功能主要是在输入输出代理模块中实现。数据监测点的设置如图 4 所示。

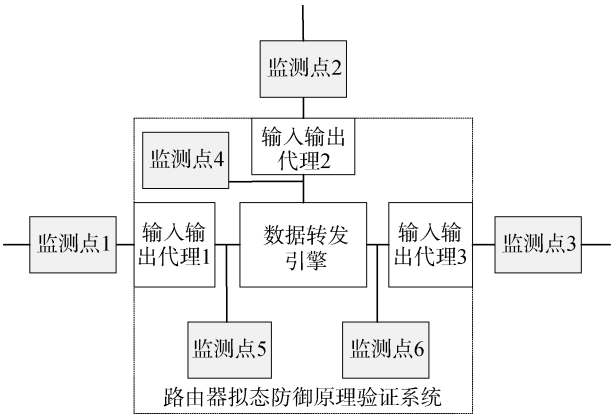

图 4 数据监测点设置方案

5.1 数据变换功能测试

该测试的目的是验证系统是否能对输入的数据报文执行数据变换操作, 并且在数据报文离开系统前执行逆变换, 从而防止利用数据平面数据流触发后门/漏洞, 导致路由器工作异常或者瘫痪。

测试方法是, 在某一线路上向被测系统发送多个数据包, 其中部分数据包具有特定的负载, 其他线路不发送任何数据。然后在发送数据的线路上的监测点记录所有流经的数据包, 同时在其他监测点监测线路上的数据包流经情况, 一旦发现有数据包通过, 则将这些数据包与其他监测点上截获的流量进行比对, 从而判断数据变换功能是否正常实现。该过程重复三次, 每次测试数据由不同的线路输入。测试结果如表 3、表 4 和表 5 所示。

表 3 数据变换功能测试结果(监测点 1 输入)

监测点编号	是否有流量经过	负载比对结果
1	有	与监测点 3 相同, 与监测点 5、6 不同
2	无	
3	有	与监测点 1 相同, 与监测点 5、6 不同
4	无	
5	有	与监测点 6 相同, 与监测点 1、3 不同
6	有	与监测点 5 相同, 与监测点 1、3 不同

表 4 数据变换功能测试结果(监测点 2 输入)

监测点编号	是否有流量经过	负载比对结果
1	有	与监测点 2 相同, 与监测点 4、5 不同
2	有	与监测点 1 相同, 与监测点 4、5 不同
3	无	
4	有	与监测点 5 相同, 与监测点 1、2 不同
5	有	与监测点 4 相同, 与监测点 1、2 不同
6	无	

表 5 数据变换功能测试结果(监测点 3 输入)

监测点编号	是否有流量经过	负载比对结果
1	无	
2	有	与监测点 3 相同, 与监测点 4、6 不同
3	有	与监测点 2 相同, 与监测点 4、6 不同
4	有	与监测点 6 相同, 与监测点 2、3 不同
5	无	
6	有	与监测点 4 相同, 与监测点 2、3 不同

从测试结果来看, 数据包进入被测系统内部, 其负载会被输入输出代理进行编码变换处理, 而在送出被测系统后, 该数据又会被实施逆变换, 从而与输入的数据负载保持一致。数据在被测系统内部成功实施数据变换。

5.2 数据流指纹功能测试

该测试的目的是验证系统对于进入系统的数据报文是否能正常施行添加数据流指纹操作, 在离开拟态路由器前执行去数据流指纹功能, 防止攻击者利用数据平面功能组件进行数据包篡改或转移。

测试方法是在某一线路上向被测系统发送多个数据包, 其他线路不发送任何数据。然后在发送数据的线路上的监测点上记录所有流经的数据包, 同时在其他监测点上检查流经的数据包里是否被插入字符串指纹, 从而判断数据流指纹功能是否正常实现。该过程重复三次, 每次测试数据由不同的线路输入。测试数据如表 6、表 7 和表 8 所示。

表 6　数据流指纹功能测试结果(监测点 1 输入)

监测点编号	是否有流量经过	是否发现字符串指纹
1	有	否
2	无	
3	有	否
4	无	
5	有	是
6	有	是

表 7　数据流指纹功能测试结果(监测点 2 输入)

监测点编号	是否有流量经过	是否发现字符串指纹
1	有	否
2	有	否
3	无	
4	有	是
5	有	是
6	无	

表 8　数据流指纹功能测试结果(监测点 3 输入)

监测点编号	是否有流量经过	是否发现字符串指纹
1	无	
2	有	否
3	有	否
4	有	是
5	无	
6	有	是

从测试结果来看, 对于进入系统的数据报文, 输入输出代理依据算法执行对每个数据包执行了加指纹操作; 在离开系统前, 输入输出代理执行了删除指纹操作。数据流指纹功能正常实现。

5.3　协议执行体随机呈现测试

该测试的目的是验证被测系统是否能正常完成执行体的选取和动态切换, 从而在完成正常的路由计算等功能的同时, 对外随机呈现。

测试方法是启动执行体的切换功能后, 每隔 10 分钟记录正在对外呈现的执行体的编号, 也就是 worker 执行体的编号, 同时向被测系统中注入路由表项, 然后通过测试仪不间断地向被测系统输入测试数据流, 在出口处监测数据流是否中断, 同时观测路由协议的更新数据包是否正常发送。Worker 执行体的默认切换时间为 5~15 分钟之间的随机值, 为了便于测试, 将切换时间设为固定值 10 分钟; 路由协议采用 OSPF, 注入 4 条路由。七个执行体编号为 A~G, 同一时间处于在线状态的 inspector 执行体设为 5 个, 这 5 个在线的执行体将按照编号顺序依次从 7 个执行体中选取, 观测时间以系统初始化完成的时间为起点进行记录。

表 9　协议执行体对外呈现观测结果

观测时间(分钟)	worker 执行体编号	Inspector 执行体编号
5	E	A、B、C、D、E
15	C	B、C、D、E、F
25	F	C、D、E、F、G
35	A	A、D、E、F、G
45	B	A、B、E、F、G
55	A	A、B、C、F、G
65	G	A、B、C、D、G
75	D	A、B、C、D、E

测试开始后, 各个观测时间点的执行体对外呈现情况如表 9 所示, 可以看出系统每个周期对外呈现的 worker 执行体都与前一个观测周期呈现的不一样, 且调度顺序随机。在向执行体注入路由以后, 各个监测点也捕获到 OSPF 协议发送的 LSA 通告。在注入测试数据流以后, 在出端口能够观测到流量, 且没有出现流量中断情况。

测试结果显示, 拟态路由器能够实现在线执行体的动态随机调度, 且流量转发和路由协议运行不受调度操作的影响。

5.4　协议执行体路由异常监测与处理测试

该测试的目的是验证系统是否能依据设定规则通过多模裁决机制判断异常, 切换异常执行体。

测试方法是启动执行体的切换功能后, 通过测试仪模拟邻居路由器, 向被测系统中注入路由表项, 同时, 通过测试仪不间断地向被测系统输入测试数据流。接下来模拟 worker 执行体被恶意入侵并修改路由, 方法是不通过中央控制器下发, 而直接向在线的执行体写入一条静态虚假路由。同时观测执行体的调度和测试流的转发情况。该过程在不同时间点重复 3 次。观测时间以系统初始化完成的时间为起点进行记录。

由表 10 的测试结果可以看出, 每次向在线的执行体注入虚假路由以后, 系统的多模裁决点立刻发现了路由表异常, 并进行了工作执行体的切换操作, 新呈现的执行体的路由表中不含有被注入的虚假路由表项。当执行体 B 被切换下线之后再次被调度到呈现状态时, 由于被测系统已经对其进行了数据清洗, 所以其路由表中不再含有被注入的虚假路由。测试过程中没有出现流量中断或流向被干扰情况。测试结果表明: 被测系统能够及时检测出路由表的异常表项, 并实施执行体调度切换操作, 切换后异常路由表项将被清除。

表 10 协议执行体动态变换测试结果

时间(分钟)	操作	观测结果
3	观测执行体呈现情况	执行体 B 为 worker
4	注入虚假路由	虚假路由被注入到执行体 B 的路由表中
5	观测执行体呈现情况	执行体 D 为 worker, 路由表不包括虚假路由
7	注入虚假路由	虚假路由被注入到执行体 D 的路由表中
9	观测执行体呈现情况	执行体 C 为 worker, 路由表不包括虚假路由
14	观测执行体呈现情况	执行体 C 为 worker, 路由表不包括虚假路由
15	注入虚假路由	虚假路由被注入到执行体 C 的路由表中
17	观测执行体呈现情况	执行体 F 为 worker, 路由表不包括虚假路由

5.5 内生流量拦截测试

该测试的主要目的是验证系统的多模裁决点是否能阻断由异常执行体主动对外发送的异常流量。

测试方法是: 假设 worker 执行体已经被攻击者恶意控制, 测试人员通过 worker 自身的网管其向发送命令, 使 worker 主动对外发起 Trivial File Transfer Protocol(TFTP)服务请求, 从而模拟漏洞或后门被触发以后路由器主动向攻击者建立连接并发送数据的过程。然后在多模裁决点两侧设立监测点, 检查该请求是否被拦截。为了进行对比, 第二次测试通过网管同时向 worker 和 3 个 inspector 执行体下发对外建立 TFTP 连接命令(目的 IP 相同), 并通过监测点观察 TFTP 请求是否被发送出去。监测点的部署方案如图 5 所示。

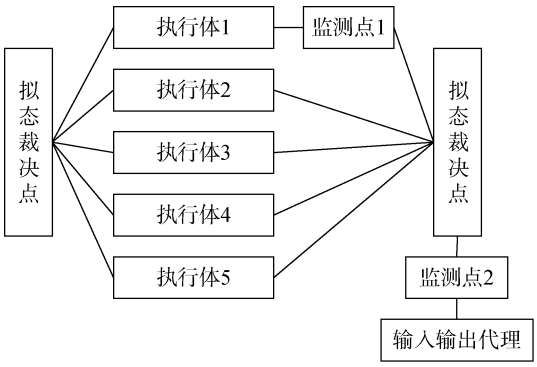

图 5 内生流量拦截测试的监测点部署方案

测试结果为: 第一次测试中, 在监测点 1 监测到 TFTP 请求的数据报文, 在监测点 2 则没有监测到 TFTP 数据报文。在第二次测试中, 在监测点 1 和监测点 2 都监测到了 TFTP 请求的数据报文。

通过测试结果可以看出, 当只有 1 个执行体向外建立连接时, 则多模裁决点会将其视为异常行为, 并拦截建立连接的请求包。当有大部分 inspector 执行体同时向外部发起连接请求时, 多模裁决点会认为这是正常行为, 并对 worker 的请求予以放行。测试结果表明, 被测系统的多模裁决机制能够有效阻止单个执行体的漏洞和后门被触发后对外发送异常报文的行为。

6 防御效果测试及结果分析

针对路由器的攻击主要分为两类[17]: 一类是针对路由协议自身机制缺陷进行的攻击, 这类攻击使得路由协议无法收敛或者产生错误的路由输出。此类攻击的目标是协议机制, 不属于被测系统的防御范围, 所以, 对此类攻击场景不进行测试。另一类攻击是针对路由器实现过程中引入的漏洞或者有目的的植入后门而发起的攻击行为。此类攻击将以获得目标控制权, 窃取情报信息、致乱或者致瘫目标系统为攻击目标, 是被测系统的主要防御对象, 防御效果测试主要围绕此类攻击场景展开。

实现过程中引入的漏洞或者后门, 对于被测系统而言, 依据其产生位置, 可以分为两类。一类位于各个执行体, 一类位于拟态插件(为实现拟态机制而引入的功能部件, 包括输入输出代理、多模裁决、动态调度等模块)。对于拟态插件而言, 其中动态调度模块单方向连接执行体, 攻击消息不可达。输入输出代理负责消息匹配转发, 多模裁决处理对象为比特流, 它们都不对数据内容或者语义做处理。因此, 无法构建针对拟态插件的攻击。同时拟态插件由于功能简单、单一, 功能代码量远小于执行体的功能代码量, 可以采用代码审计的方法进行安全评估与测试。因此, 本文主要针对执行体上存在的漏洞或者后门进行防御效果测试。

6.1 攻击模型与测试场景

依据被测系统的防御目标, 攻击者利用漏洞对路由器发起攻击的一般性攻击链如图 6 所示。

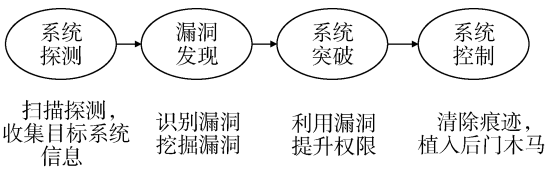

图 6 路由器漏洞利用攻击链

攻击者首先通过扫描探测的方法, 确认目标路由器的相关信息, 例如设备型号、操作系统版本、周

围网络拓扑情况、开放端口号、启动的网络服务等信息。基于扫描探测信息识别目标路由器上存在的漏洞, 然后利用漏洞进行权限提升。在提权后, 可以修改路由器的 Access Control List(ACL)规则等, 打开恶意流量进入内部网络大门; 也可以修改路由表、部署隐蔽通道, 对经过路由器的所有数据实施嗅探和中间人攻击。更进一步, 可以在路由器系统上设置后门, 进行长期持续的隐蔽控制。

分析上述攻击链, 可以看出攻击链前一环节的成功是后续环节开展的前提。为了覆盖攻击链的所有环节, 评估拟态机制对斩断攻击链各个环节的效果, 本节采用开放配合型测试方法对拟态路由器的防御效果进行测试分析, 即分别对攻击链每一环节进行逐项测试, 每个环节的测试假定攻击者已经完成该环节在攻击链中的前序步骤。

6.2 系统信息扫描测试

系统信息扫描是攻击者进行网络攻击所进行的第一步操作, 检测目标系统开放的端口、启动的服务以及操作系统版本等信息, 决定后续攻击所采用的方法手段和工具。本小节测试的目的是验证系统对于攻击链第一步的防御能力。

测试方法是采用 Nmap 工具对系统进行 10 次扫描, 每次扫描的开始时间是随机选定的, 从扫描开始一直到返回扫描结果视为一次扫描。在扫描过程中系统执行体采用随机调度方法进行调度切换。

由于这 10 次得到的结果基本类似, 选择其中一次扫描结果进行分析。扫描结果如图 7 所示, 这次扫描持续了 904 秒, 通过开放的端口号、端口上的服务来确定这是一台路由设备, 型号为 ZXR10 路由器。通过查看目标系统的调度日志得知, 在扫描过程中共有三个执行体轮流上线, 依次为中兴执行体、Cisco 执行体和 Quagga 执行体。因此, Nmap 扫描得到的最后的测试结果实际上不是对同一个目标进行扫描探测得到结果, 基于这些结果做出的测试结论必然是不准确的。汇总这 10 次扫描结果, 每次得到的结果都是不一致的, 也就是说扫描测试结果具有不可预测性。

拟态路由器的工作机制决定了它同时运行多个执行体, 并进行随机调度对外呈现, 使得系统对外呈现的信息发生了跳变, 仅仅凭借一两次扫描探测难以准确识别目标系统的相关信息。为了获得准确的目标信息, 攻击者将不得不增加扫描探测的次数和频度, 这将明显增加攻击成本。如果扫描探测频次过高, 就很容易被安全检测设备或者通过日志分析发现。所以, 在扫描探测阶段, 拟态防御机制可以有效的迷惑攻击者, 明显降低攻击者获取目标系统信息的准确度, 增加扫描探测花费的时间, 显著提升了攻击者获取目标系统信息的难度。

```
PROTOCOL STATE         SERVICE
1        open          icmp
2        open|filtered igmp
4        open|filtered ipv4
6        open          tcp
17       open          udp
41       open|filtered ipv6
46       open|filtered rsvp
47       open|filtered gre
89       open|filtered ospfigp
103      open|filtered pim
112      open|filtered vrrp

PORT     STATE         SERVICE VERSION
23/tcp   open          telnet
161/udp  open          snmp    SNMPv1 server; nil SNMPv3 server (public)
| snmp-sysdescr: ZXR10 ROS Version V4.6.03b GER Software,
| Version V2.6.03b41 Copyright (c) 2000-2005 by ZTE Corporation Compiled Jul
520/udp  open|filtered route
1701/udp open|filtered L2TP
Network Distance: 1 hop
Service Info: Host: ZXR10
```

图 7 系统信息扫描探测结果

6.3 系统漏洞发现测试

上节测试过程中, 通过 Nmap 扫描探测并未确定目标系统的具体信息, 但是可以基本明确系统开放了哪些端口, 运行了哪些服务协议。本小节测试目的是在上节系统信息扫描的基础上, 对这些开放的服务做进一步的漏洞扫描, 测试验证系统中固有漏洞或者后门的呈现性质。

测试方法是采用 Nessus 工具对目标系统的几个服务进行漏洞扫描, 共进行 10 次扫描。

测试结果仅 1 次发现了目标系统存在高危脆弱点, 结果如表 11 所示。该高危脆弱点为 SNMP 协议的 public 团体字。这是因为系统中有一个执行体使用了 public 团体字。由于系统动态性的存在, 其他执行体并没有采用这种易猜的团体字, 所以, 在 10 次扫描过程中仅有 1 次发现目标系统存在该脆弱点。

表 11 漏洞扫描结果

漏洞级别	漏洞数量	漏洞明细
Critical	0	
High	1	SNMP Agent Default Community
Medium	0	
Low	1	Unencrypted Telnet Server

漏洞扫描是攻击者实施攻击第二步, 该阶段的结果将决定了后续攻击手段、工具和攻击的难易程度。如果扫描到目标系统存在漏洞, 那么攻击成功的概率将会大增。系统通过随机调度机制, 多个执行体以跳变的形式对外呈现, 使得漏洞扫描工具面

向变化的目标，很难在短时间内准确得到目标系统的漏洞信息。因此，拟态防御机制可以在不消除系统漏洞或脆弱点前提下改变漏洞或系统脆弱点的呈现特性。

6.4 系统漏洞利用难度测试

本小节的测试目的是评估验证系统中视在漏洞的利用难度。跳过攻击链的前序环节，我们直接假定攻击者已经获知目标系统存在一个可利用漏洞，在此基础上，利用该漏洞发起攻击，验证系统的防御效果。

测试选用思科 IOS 的 SNMP 漏洞，该漏洞存在于系统的思科执行体上，该漏洞被利用后会启动 TFTP 服务，允许攻击者通过 TFTP 下载目标系统的配置文件。测试方法是，首先暂停系统的动态调度和多模裁决机制，即关闭系统的拟态防御机制，并设定思科执行体为 worker，此时可以认为系统等价于一台思科路由器，在该条件下验证漏洞的可利用情况。然后恢复系统的动态调度和多模裁决机制，即启用拟态防御，再次验证该漏洞的可利用情况。测试结果如下:

关闭拟态机制的情况下，利用 Metasploit 工具对系统进行渗透攻击，得到结果如图 8 所示，可以看到该漏洞可被成功利用，利用该漏洞可以获得目标系统的 enable 口令，以及相应的系统配置文件。在 60 分钟内，每隔 180 秒，发起一次上述攻击，均得到相同结果。

```
msf auxiliary(cisco_config_tftp) > exploit
[*] Starting TFTP server...
[*] Scanning for vulnerable targets...
[*] Trying to acquire configuration from 1.1.1.66...
[*] Scanned 1 of 1 hosts (100% complete)
[*] Providing some time for transfers to complete...
[*] Incoming file from 1.1.1.66 - 1.1.1.66.txt 860 bytes
[*] Saved configuration file to /home/1.1.1.66.txt
[+] 1.1.1.66:161 Unencrypted Enable Password: !qaz@wsx
[*] Collecting :!qaz@wsx
[+] 1.1.1.66:161 Username 'nmgdcy' with Password: n@Qos$mpls
[*] Collecting nmgdcy:n@Qos$mpls
[+] 1.1.1.66:161 SNMP Community (RO): nmgdcy@demaxiya
[*] Collecting :nmgdcy@demaxiya
[+] 1.1.1.66:161 SNMP Community (RW): public
[*] Collecting :public
[*] Shutting down the TFTP service...
[*] Auxiliary module execution completed
```

图 8 关闭拟态机制时的漏洞利用结果

开启拟态机制的情况下，重复上述过程，发现漏洞始终无法被成功利用。这是由于拟态路由器采用的多模裁决机制，攻击者通过漏洞触发的 TFTP 数据流是个体行为(针对同一个 TFTP 输入仅有一个执行体进行响应)，与其他执行体的响应行为不一致，因此无法通过裁决点，漏洞利用失败。

漏洞的触发利用是攻击者实施攻击的核心步骤，可以说，漏洞能否被成功触发是评价一个系统安全性的最终指标。因此，拟态防御机制能够在不消除系统漏洞前提下，大幅增加系统视在漏洞的可利用难度。

6.5 系统后门利用难度测试

本小节测试目的是评估系统中后门的利用难度，测试拟态防御机制对于后门攻击的防御能力。

从保障信息系统安全角度来说，可以利用后门进行系统致瘫以破坏可用性、信息获取以破坏机密性、系统致乱以破坏完整性。所以，测试例分别围绕这三个方面进行设置。

测试前在系统执行体中内置后门，测试方法与上一小节类似，首先关闭系统的拟态防御机制，并将后门所在执行体设定为 worker，在该条件下验证后门的可利用情况；然后启用系统拟态防御，再次验证该后门的可利用情况。本节测试采用图 3 的网络拓扑。

(1) 致乱后门

为了验证对致乱后门的防御效果，在执行体上进行了后门设置，该后门特征为: 如果收到的 OSPF 协议 hello 报文中 Neighbor 字段含有 0x5a5a5a02 值，则后门被触发，执行体自动增加一条到 A.B.C.D 的缺省路由，并使得其它路由无效，其中 A.B.C.D 由 hello 报文中的 Designated Router 字段指定。

在关闭拟态机制条件下，测试仪发向路由器接口 1 的数据被从接口 2 正确转出。测试方通过接口 4 发送后门触发报文，触发后门，原本从接口 2 发出的数据，被修改为从接口 3 转出。通过 SNMP 可以查看到执行体中被自动添加了一条下一跳为 192.168.3.100 的默认路由，如图 9 所示。说明后门被成功触发并被利用。

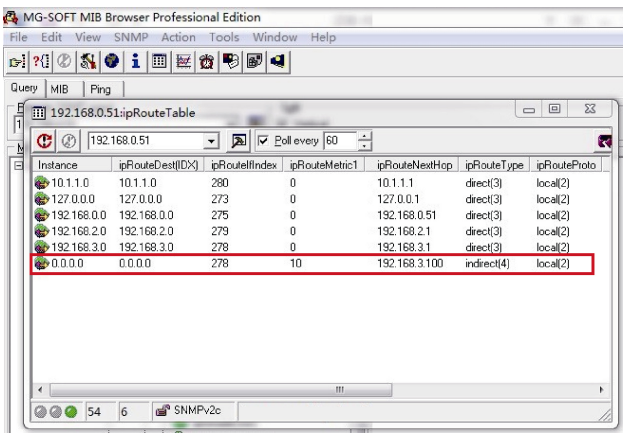

图 9 关闭拟态机制时路由表篡改后门的利用结果

在开启拟态机制后，重复上述后门触发操作，通过 SNMP 仍然可以看到后门执行体生成了默认路由，说明执行体后门已被触发。但是，并未发现数据流向的改变。这说明系统后门可被触发，但未被成功利用。

分析本次结果，拟态防御机制启动以后，路由表篡改的后门无法成功利用。这是由于拟态防御机制的多模裁决特性决定的。攻击者通过触发后门修改的路由表只存在单个执行体上，与其他在线执行体的路由表不一致，因此无法通过裁决点，路由表篡改失败。

(2) 窃情后门

为了验证对窃情后门的防御效果，在执行体上进行了后门设置，该后门特征为：执行体收到特定的 SNMP 触发报文后，自动将内部路由表信息每隔 30 秒以 UDP 报文发送给指定 IP 地址，该 IP 地址由 SNMP 触发报文指定。

在关闭拟态机制条件下，测试方通过接口 4 发送后门触发报文，之后测试仪在接口 3 上收到了原目端口号为 8993 的 UDP 报文，如图 10 所示。经查验其载荷部分携带的信息与执行体的路由表一致。说明后门被成功触发并被利用。

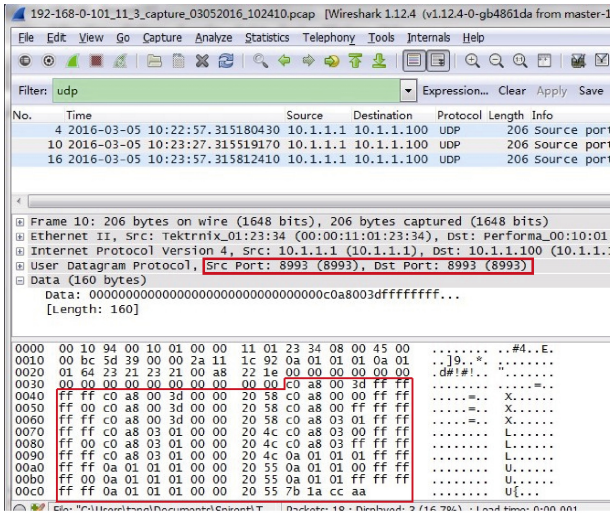

图 10　关闭拟态机制时窃情后门利用结果

在开启拟态机制后，重复上述后门触发操作，测试仪在接口 3 上一直未收到原目端口号为 8993 的 UDP 报文，这说明拟态机制使得后门无法被成功利用。

从本次测试结果可以看出，拟态防御机制启动以后，窃情后门无法被成功利用，与路由表篡改后门相同，这也得益于多模裁决特性，后门所在执行体向外部发送的 UDP 报文同样是个体行为，会在裁决点被发现，无法送出。

(3) 致瘫后门

为了验证对致瘫后门的防御效果，在数据转发平面人为植入后门，该后门特征为：当收到源、目的端口号为 66535 且载荷为全 F 的 UDP 报文后，系统瘫痪，转发功能失效。

在关闭拟态机制条件下，测试仪发向路由器接口 1 的背景流量数据被从接口 2 正确转出。之后，在接口 1 上叠加发送后门触发报文，发现测试仪的接口 2 收不到任何报文。通过串口查看转发单元，发现其对任何命令均没有响应。说明后门被成功触发并被利用。在开启拟态机制后，重复上述后门触发操作，测试仪在接口 2 上一直能够收到背景流量和后门触发报文，这说明拟态机制使得后门无法被成功利用。

从本次测试结果可以看出，拟态防御机制启动以后，致瘫后门无法被成功利用，这得益于转发平面的负载语义变换功能，通过对进入到转发平面的数据负载进行动态变换，使得基于特殊比特流进行硬件逻辑触发的后门无法工作。

通过对上述三个测试例的测试结果分析，可以得出以下结论，拟态防御通过引入动态异构冗余以及多模裁决机制，能够在不消除系统后门前提下，大幅提升基于后门的攻击难度。

7　总结

路由器是网络空间中最为重要的基础核心设备，由于其封闭性，导致存在大量未知漏洞和后门，使其成为了攻击者的重要攻击目标。由于传统被动防御方法的局限性，难以应对未知漏洞和后门。拟态防御机制采用主动防御技术，被引入到路由器的架构设计中，成为了路由器安全研究的发展方向。本文介绍了路由器拟态防御原理验证系统的实现思路，提出了针对引入拟态防御机制的路由器测试方法，并以该方法为指导，对路由器拟态防御原理验证系统进行了全面的测试。测试结果表明，路由器拟态防御原理验证系统能在不影响基础性能的前提下，实现了拟态防御机制的核心功能，并对基于未知后门或漏洞的攻击进行有效阻断和防御，大幅提升了自身的安全防护能力，证明拟态防御机制的有效性。同时本文涉及的测试方法和手段，为拟态机制测试规范或标准的制定提供了一定的参考价值。

致　谢　国家信息技术安全研究中心、中国信息通信研究院、中国电子设备与系统工程研究所、北京奇虎科技有限公司、启明星辰信息安全技术有限公司、安天科技股份有限公司等单位在测试实施过程

中付出了大量时间和精力, 在此一并致谢!

参考文献

[1] Z.Y.Shao, L.L.Jiao, “prism doors Refracting the developing direction of industrial software,” China Information: e Manufacturing, 2013, vol. 11, pp.24-33
(邵泽宇, 皎丽丽. “‘棱镜门’折射我国工业软件何去何从,” 2013, 11:24-33.)

[2] “About the presence of a variety of preset router backdoor vulnerability briefing,” http://www.cert.org.cn/publish/main/9/2014/2014 042912193838368446 4/2014042912193838368446 4_.html, 2016.9
(关于多款路由器设备存在预置后门漏洞的情况通报, http://www.cert.org.cn/publish/main/9/2014/2014 0429121938383684464/20140429121938383684464_.html, 2016.9)

[3] Y. Wang. “Cyber Active Defense and Active Defense Network.” Secrecy Science and Technology, 2014,vol.11, pp.006
(王宇, “网络主动防御与主动防御网络”, *保密科学技术*, 2014, 11: 006.)

[4] X.F.Gao, P. Shen. “Active Defense Technology for Cyber Security.” Computer Security. 2009, vol. 1, pp. 66.
(高晓飞, 申普兵, “网络安全主动防御技术”., *计算机安全*, 2009, 1: 66.)

[5] S. Jajodia, A.K. Ghosh, V. Swarup, C. Wang, XS Wang, “Moving Target Defense: Creating Asymmetric Uncertainty for Cyber Threats,” Springer Ebooks (2011).

[6] R. P. Guidorizzi, “Security: Active authentication.” IT Professional, 2013 (4), pp. 4-7.

[7] J.X.Wu, “mimic securiy defence of cyberspace,” *Secrecy science and technology*, 2014(10)
(邬江兴, “网络空间拟态安全防御,” *保密科学技术*, 2014(10))

[8] J.X.Wu, “Meaning and vision of mimic computing and mimic security defense,” *Telecommunications science*, 2014, 30(7): 1-7
(邬江兴, “拟态计算与拟态安全防御的原意和愿景,” *电信科学*, 2014, 30(7): 1-7)

[9] Industry and Information Technology of the People’s Republic of China, “YD/T 1097-2009 Equipment Technical specification Core router”, 2009.
中华人民共和国工业和信息化部, ”YD/T 1097-2009 路由器设备技术要求 核心路由器”, 2009.

[10] N.Li, Z.H.Li “Research and practice of software test policies based on blackbox testing”, Application Research of Computers, 2009, 26(3): 33-37
(李宁, 李战怀, “基于黑盒测试的软件测试策略研究与实践”, *计算机应用研究*,2009,26(3):33-37)

[11] Z.Z.Zhang, Z.Y.Chen, B.W.Xu, “Research Progress on Test Case Evolution”, Journal of Software, 2013, 24(4): 663-674
(张智轶, 陈振宇, 徐宝文,” 测试用例演化研究进展”, *软件学报*, 2013, 24(4): 663-674)

[12] “Wireshark”, https://www.wireshark.org/, 2016.10

[13] G. Lyon. “Nmap security scanner,” http://namp.org, 2016.10

[14] “Nessus. Tenable Network Security”. http://www.tenable.com/products/nessus-vulnerability-scanner. 2016.10

[15] Metasploit. https://www.metasploit.com. 2016.10

[16] Moy, J., “OSPF Version 2”, STD 54, RFC 2328, DOI 10.17487/RFC2328, http://www.rfc-editor.org/info/rfc2328,1998.4

[17] A.V. Andrew, V. G. Konstantin and N.V. Janis, “Exposing Cisco Network Hackinng,” Tsinghua University Press, 2008
(A.V. Andrew, V. G. Konstantin and N.V. Janis, “思科网络黑客大曝光”, 清华大学出版社, 2008)

马海龙 于 2011 年在信息工程大学通信与信息系统专业获得博士学位。现任信息工程大学信息技术研究所副研究员。研究领域为网络安全、路由工程。研究兴趣包括: 创新网络体系、网络安全管控等。Email: longmanclear@163.com

江逸茗 于2014年在信息工程大学通信与信息系统专业获得博士学位。现任信息工程大学信息技术研究所助理研究员。研究领域为新型网络体系结构、网络空间安全防御。研究兴趣包括: 网络虚拟化等技术。Email: j8403@163.com

白冰 于 2007 年在国防科技大学通信与信息系统专业获得硕士学位。现任信息工程大学信息技术研究所助理研究员。研究领域为网络安全、路由工程。研究兴趣包括: 网络管理技术、网络安全防护技术等。Email: bb_nudt@126.com

张建辉 于2011年在信息工程大学通信与信息系统专业获得博士学位。现任信息工程大学信息技术研究所副研究员。研究领域为宽带信息网路。研究兴趣包括: 路由转发技术、网络安全管控等。Email: ndsczjh@163.com