

SDN 中基于历史信息的负反馈调度算法

吕迎迎, 郭云飞, 王禛鹏, 程国振, 王亚文

(国家数字交换系统工程技术研究中心, 河南 郑州 450002)

摘要: 在当前 SDN 架构中, 控制器遭受着很多潜在的攻击, 如恶意流规则等可能会引入虚假的流规则使主机混乱。基以此, 提出一种基于历史信息的负反馈调度算法, 利用假设检验对攻击者的行为进行判断, 并将此作为调度的依据。仿真实验结果和分析表明, 相比于传统调度方法, 所提算法在一定程度上可以增加攻击者的时间成本, 从而有效防御攻击者的探测攻击, 而且控制器种类越多, 系统越难被攻破。

关键词: 动态异构冗余; 负反馈; 主动防御

中图分类号: TP393

文献标识码: A

doi: 10.11959/j.issn.2096-109x.2018047

Negative feedback scheduling algorithm based on historical information in SDN

LYU Yingying, GUO Yunfei, WANG Zhenpeng, CHENG Guozhen, WANG Yawen

National Digital Switching System Engineering & Technological R&D Center, Zhengzhou 450002, China

Abstract: In the current SDN architecture, the controllers suffer from lots of potential attacks. For example, malicious flow rule attacks may introduce fake flow rules to confuse the host. A negative feedback scheduling algorithm based on historical information was proposed, in which hypothesis testing was used to judge the behavior of the attacker and the result will be used as a basis for scheduling. Simulation results and analysis show that, compared with the traditional scheduling methods, the proposed algorithm can increase the attacker's time cost to a certain extent, so as to effectively defend the attacker's probe attack. In addition, the more types of controllers, the more difficult it is to break the system.

Key words: dynamic heterogeneous redundancy, negative feedback, active defense

1 引言

近年来, 随着网络的普及, 人们的生产生活甚至国家的安全发展对网络空间越来越依赖, 网络空间的重要性日益突出。但是, 网络空间的脆弱性使不法分子有机可乘, 网络犯罪、黑客攻击等对国家安全的威胁凸显^[1]。网络空间的攻防态势处于一种信息不对称的状态, 攻击者可以决定何时何地攻击, 而防御者只能被动防御^[2]。而且被动防御技术难以应对未知漏洞、后门等问题,

收稿日期: 2018-04-28; 修回日期: 2018-05-17

通信作者: 吕迎迎, yyl1994@pku.edu.cn

基金项目: 国家自然科学基金创新研究群体基金资助项目 (No.61521003); 国家重点研发计划基金资助项目 (No.2016YFB0800100, No.2016YFB0800101); 河南省科技攻关计划基金资助项目 (No.172102210615); 国家自然科学基金资助项目 (No.61602509)

Foundation Items: The Foundation for Innovative Research Groups of the National Natural Science Foundation of China (No.61521003), The National Key R&D Program of China (No.2016YFB0800100, No.2016YFB0800101), The Key Technologies Research and Development Program of Henan Province (No.172102210615), The National Science Foundation of China (No.61602509)

因而主动防御技术逐渐发展并成为网络安全研究的重点。

入侵容忍^[3]、移动目标防御^[4]和拟态防御^[5]是3种典型的主动防御技术。入侵容忍技术是由容错技术发展而来,入侵容忍技术的主要目标是数据完整性、数据机密性以及服务可用性^[6]。移动目标防御是不断地进行动态变化来迷惑攻击者,意图增加攻击者的攻击成本,达到降低其攻击成功率的目的^[7]。而拟态防御是由郭江兴院士提出的“改变游戏规则”的新途径,动态地利用异构冗余的组件,使未知漏洞和后门等无法准确地确定其环境,无法构建成功攻击链,以达到降低系统风险的目的^[8]。

网络侦察IP地址和端口是许多主机和网络攻击的先决条件^[9]。本文利用异构冗余的架构,提出一种基于历史信息的负反馈调度算法用以“净化”NOS池,达到有效防御攻击者攻击的目的。

2 相关工作

现在已有很多关于NOS安全的研究,大体上分为三类。第一类是在已有的特定控制器的基础上,改进现有的安全模块的设计。例如, FortNOX^[10],它在开源NOX的基础上增加了一个安全策略实施模块,在一定程度上可以较好解决流规则检测与冲突的问题。与FortNOX类似,文献[11]在开源Floodlight的基础上设计了一个安全增强版的控制器——SE-Floodlight,它的安全执行内核由一组特定的安全应用程序管理模块构成。还有一种方法是在设计NOS之初就将安全纳入考虑,并且将其作为需要解决的核心问题。PANE^[12]是由Ferguson等设计开发的一种安全型NOS,它主要用于解决与脆弱用户间请求冲突的问题。而Shin等^[13]将重点放在控制层的弹性问题上,设计开发出Rosemary,用以应对第三方网络应用程序中潜在的漏洞、致命的脆弱性和恶意逻辑。

第二类是在控制器的基础上设计并部署可组合的安全模块库,通过各类安全组件之间的协同工作来检测及消除安全威胁。FRESCO^[14]提供了一种单击触发的编程框架,使安全研究人员可以实现共享及组合多个不同的安全检测

和防护模块。

现在越来越多研究人员关注分布式控制器,以避免单个控制器发生单点故障^[15]。第三类便是从多控制器的角度出发,设计具有一定弹性的分布式控制器架构。ONOS^[16]是一种开放式网络操作系统,通过采用分布式架构实现了高可用性和高扩展性,它的多备份NOS的设计大大增加了系统的容错能力,即便主控制器发生瘫痪等故障,ONOS也可以自动切换至备份控制器以保证网络的平稳运行。文献[17]借助拜占庭容错机制,实现了一种能有效防御针对SDN控制层攻击的NOS系统。该系统中,交换机由多个控制器共同控制,其流表的更新是由多个控制器共同决定的。文献[18]在网络操作系统中引入动态、异构及冗余的拟态基因来构建顽健的系统架构并提高内部行为的不可预测性,从而增加外界攻击者对内部架构与运行机制的探测难度与认识困境,提升系统的安全性能。类似地,文献[19,20]也提出了一个SDN安全体系架构,利用多控制器的异构性与冗余来加强架构的安全性,还引入了动态调度机制进一步提高其性能,使系统在面临威胁时做出最佳应对改变。

3 问题描述

拟态防御通过动态异构冗余架构(DHR, dynamic heterogeneous redundancy)来破坏攻击信息链,从而增加网络攻击的难度和成本,降低未知漏洞及后门带来的网络威胁,达到保护网络安全的目的。

DHR架构^[5]由异构组件池、异构执行体池、动态选择算法、输入代理、执行体集和表决器组成。如图1所示,由异构组件构成 m 个功能等价的异构执行体,按策略调度算法动态地从执行体池选出 n 个执行体构成一个执行体集($A_1, A_2, \dots, A_n$),该架构中的输入代理将输入转发给当前执行体集中的各个执行体,这些执行体的输出提交给表决器进行判决,最后得到系统的输出。

在该架构中,不仅被调用的执行体会遭受攻击者的探测攻击,处于待机状态的执行池中的执行体也一直面临着攻击者的威胁,而系统的正常运行与执行体池的整体安全性息息相关。如果执

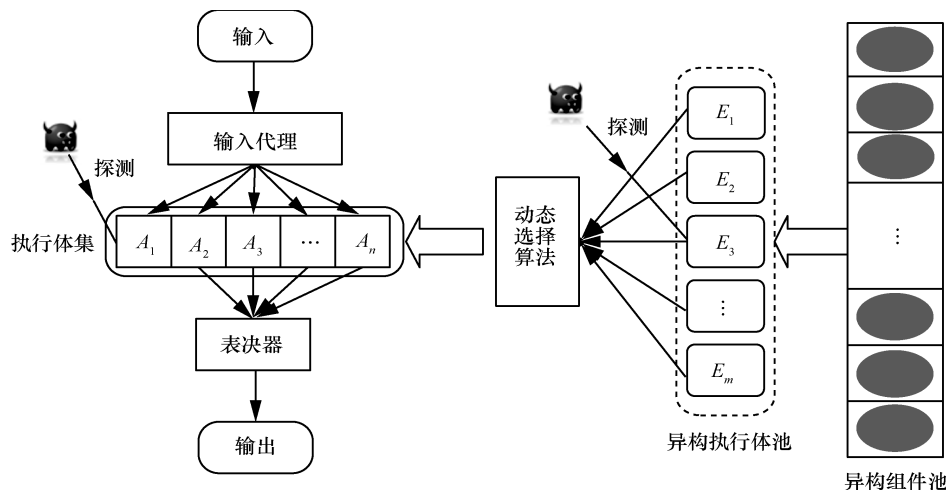


图1 DHR 架构

行体池系统中的执行体被攻破，那么系统的安全很难得到保证。

一旦攻击者存有历史探测信息，若其攻破某一类型执行体，那么在这之后攻击者要攻破相似的执行体需要花的时间将大大减少。而且，若某执行体正在被攻击，其被攻击的次数越多，它就越危险，如果不考虑待机的执行体安全，任由攻击者不断进行尝试探测攻击，那么执行体迟早会被一一攻破，最终整个系统也会瘫痪。

因此，本文通过对系统运行过程中的历史信息进行分析，设计了一种基于历史信息的负反馈调度算法，以此来减小脆弱执行体被调用的概率，从而规避攻击者探测攻击对系统的威胁。

4 负反馈调度策略

假定攻击者进行攻击是有目的性有针对性

的，不是盲目的，那么攻击者在进行探测攻击时必然有一定的规律，因此，可以通过对统计数据进行分析得到探测的规律。加入负反馈的 DHR 架构如图 2 所示。

4.1 模型建立思路

一般认为，在执行体集中，被攻破的 NOS 数量小于被选调 NOS 数量的 $\frac{1}{2}$ 。可以把整个异构

NOS 池中的 NOS 分为两大类，如图 2 所示，分别是被调用的执行体类 A ， $A = \{A_1, A_2, \dots, A_m\}$ ，以及未被调用的执行体类 B ， $B = (B_1, B_2, \dots, B_n)$ 。其中， $A_1, A_2, \dots, A_m$ ， $B_1, B_2, \dots, B_n$ 是异构的 NOS 组，而且每个 NOS 均有各自的 IP 地址。因此，可以通过以下方法判断出是哪一类 NOS 受到了攻击。若 A 中的 NOS 被攻破，那么可以通过表决器的输出结果来判断识别出具体哪个 NOS 被攻击成功；若 B 中的 NOS 被攻击，那么可以抓

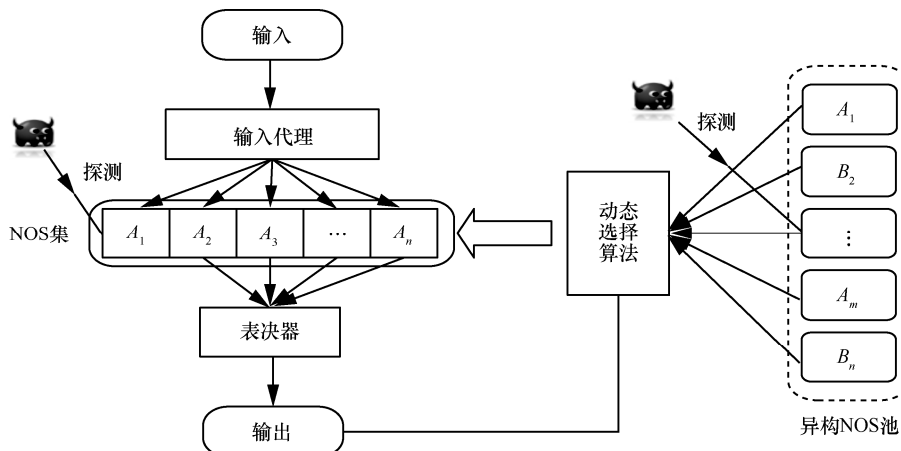


图2 加入负反馈的 DHR 架构

包查看是否有流量到非调用 NOS 所属的 IP 地址。同时, 选调器可以根据输出进行调节, 在之后做出更有效的调度。

4.2 理论分析

为了快速准确地表征出攻击扫描策略, 观察由系统监测得到的探测数据并使用统计假设检验估计它们的分布。为此, 引入 2 个基本假设, 即非一致性检验和非重复检验。通过这 2 个检验分析攻击者的行为并据此做出规避攻击的行为。

第一个假设采用的是非一致性检验, 如果该假设被验证为真, 则将其表示为非均匀攻击, 旨在确定攻击者是否在有针对性地攻击某类 NOS, 这样可以将选调器调用该类 NOS 的概率降低甚至不选用该类 NOS 来规避攻击者的有效攻击; 第二个假设采用的是非重复检验, 如果该假设被验证为真, 则将其表示为非重复攻击, 旨在确定攻击者是否以相同概率攻击不同类 NOS。这样可以以相同概率调用各类 NOS 来规避攻击者的有效攻击。

下面分别对定义的这 2 类攻击进行介绍。

1) 非均匀攻击

为了确定攻击者是否在进行非均匀攻击, 需要对统计的数据进行非一致性检验。

该检验的目的是为了确定攻击者以非等概率的机会攻击各类 NOS, 即攻击的频率分布与均匀分布不一致, 可以采用皮尔逊 χ^2 检验法^[21]。假设得到 z 个观测值, χ_k 表示 NOS 类 r_k 被攻击的次数 ($r_k \in \Omega$), z 表示攻击的总次数, N 为 NOS 类的总数, 那么 $\frac{z}{N}$ 为所有 NOS 类被攻击的平均次数。则观察 z 事件后的拟合优度值 χ_z^2 的计算式为

$$\chi_z^2 = \sum_{k=1}^N \frac{\left(x_k - \frac{z}{N}\right)^2}{\frac{z}{N}} \quad (1)$$

本文认为显著性水平 $\alpha = 0.05$, 将上述 χ_z^2 值与 $N-1$ 自由度的卡方分布进行比较确定拟合优度。当 χ_z^2 概率不大于 0.05 时, 该检验接受零假设, 即

$$P(\chi_z^2) \begin{cases} \leq 0.05, \text{接受零假设} \\ > 0.05, \text{拒绝零假设} \end{cases} \quad (2)$$

接受零假设, 意味着观测值与均匀分布的偏差非常显著, 也就是说, 潜在攻击者在集中扫描某些 NOS 类的 IP 地址, 那么防御者可以降低调用该类 NOS 的概率或不调用该类 NOS 来增加攻击者攻击成功的难度, 甚至还可以利用蜜罐技术, 布置蜜罐 NOS 来代替被攻击的 NOS, 从而化被动为主动, 更好地掌握攻击者的动作及信息。

2) 非重复攻击

为了确定攻击者是否在进行非重复攻击, 对统计的数据进行非重复检验。该检验的目的是为了确定攻击者尽量避免重复对同一类 NOS 进行探测或者最小化其探测次数。为了检验该假设, 可以根据统计的数据计算得到各类被扫描 NOS 的平均次数的变异系数。假设 χ_i 表示第 i 类 NOS 受到扫描的次数, z 表示 NOS 类被扫描的总次数, N 表示 NOS 类的总数。此外, 假设当得到 z 个观测值时, $\overline{\chi^z}$ 为各 NOS 类被扫描的平均次数, 那么在接收到第 $z+1$ 次扫描时, 有

$$\chi_k = \chi_k + 1 \quad (3)$$

而各 NOS 类被扫描的平均次数可以用下列公式进行计算。

$$\overline{\chi^{z+1}} - \overline{\chi^z} = \frac{z+1}{N} - \frac{z}{N} = \frac{1}{N} \quad (4)$$

即

$$\overline{\chi^{z+1}} = \overline{\chi^z} + \frac{1}{N} \quad (5)$$

令二阶矩 $M_{2,z} = \sum_{i=1}^N (\chi_i - \overline{\chi^z})^2$, 那么有

$$M_{2,z+1} = M_{2,z} + 2\chi_k - \overline{\chi^z} - \overline{\chi^{z+1}} + 1 \quad (6)$$

则该样本的无偏方差为

$$S_{z+1}^2 = \frac{M_{2,z+1}}{N-1} \quad (7)$$

那么变异系数 c_v 为

$$c_v = \frac{\sigma}{\mu} = \frac{S_z}{\overline{\chi^z}} \quad (8)$$

当 c_v 不大于 0.001 时, 接受该检验, 这意味着攻击者在以相同概率扫描不同类 NOS, 因此可以以相同的概率随机调用各类 NOS, 以此来防御攻击者的探测攻击。

4.3 负反馈调度算法

前文对定义的 2 类攻击进行了细致的理论分

析, 为了得到可信的数据, 需要记录每次被探测的详细情况, 如执行体是哪一类 NOS、NOS 类被探测次数等, 为方便查询, 可以利用表 1 记录所有 NOS 类的相关状态信息。

表 1 NOS 类状态信息		
编号	NOS 类型	探测次数
1	Floodlight	χ_1
2	Ryu	χ_2
...	...	...
k	ONOS	χ_k
...	...	...
n	OpenDaylight	χ_n

每当异构 NOS 池的 NOS 类被探测或有反馈 NOS 集中的 NOS 被攻击时, 则将表 1 更新, 也就是说, 如果有 NOS 类被探测, 则将表中相应的探测次数加 1。如此, 可以根据统计得到的信息进行相应假设检验, 提出基于历史信息的负反馈调度算法。其根本是利用假设检验, 对攻击者的扫描探测行为进行分类, 根据分类结果做出合适调度, 以此来对抗攻击者。

下面对该算法的初始化及调度流程进行描述。

初始化: 首先根据 NOS 类的类型将 Ω 分为 n 类, 而且 NOS 类状态信息表中所有 NOS 类的探测次数均为 0, 最初的 NOS 集是由调用的 NOS 类中的第一个 NOS 组成, 即 $A_{11}, A_{21}, \dots, A_{m1}$ 。

调度流程: 系统的调度是由表决器的判决信息和监测信息决定的, 只有在分析二者相关信息发现异常之后系统才会进行改变, 这样可以避免频繁切换导致开销过大, 同时, 也只对异常 NOS 类进行调整, 这样可以减少每次调整需要切换的次数。

具体调度流程伪代码如下。

算法 1 调度流程伪代码

1) $\Omega = U_{k=1}^n r_k$; //按类型区别将所有 NOS 类分为 n 类

2) $\Omega = U_{i=1}^m A_i + U_{j=1}^{n-m} B_j$; //NOS 类由 A 和 B 组成

3) $A_{cur} = \{A_{11}, A_{21}, \dots, A_{m1}\}$ //NOS 集默认由每类 NOS 中首个组成

4) $\chi_1 = \chi_2 = \dots = \chi_n = 0$

5) for $i=1$ to m do

6) if $A_i \leftarrow$ 表决器反馈消息 do

7) $\chi_i = \chi_i + 1$

8) end if

9) end for

10) for $j=1$ to $n-m$ do

11) if $B_j \leftarrow$ 抓包存在流向该 NOS 类的流量 do

12) $\chi_j = \chi_j + 1$

13) end if

14) end for

15) Test $(\chi_1, \chi_2, \dots, \chi_n)$; //对统计数据进行假设检验

16) if 非均匀攻击 do

17) set 阈值 k ;

18) find $\chi_i > k, \chi_j > k$, 记为集合 A_f 和 B_f , 总数分别为 x, y ;

19) $A_{cur} = A_{cur} - \{A_f\} + \{U_{j=1}^x (B_j)\}$, 其中 $B_j \subseteq B - B_f$;

//剔除选出的 NOS 类, 并从待机的 NOS 类中选出等量 NOS

20) end if

21) if 非重复攻击 do

22) $A_{cur} = random_choose(r)$; //以相同概率选取 NOS 类

23) end if

24) end if

5 仿真实验与结果分析

本节通过仿真实验对所提基于历史信息的负反馈调度算法的有效性进行评估。仿真实验中, 选用 5 类不同的 NOS, 且每类 NOS 都有 3 个实例。为了进行对比, 将本文方法与 2 种调度策略进行对比, 第一种是传统 SDN 架构中的静态结构, 即不切换, 对反馈

结果不做反应；第二种是以选取系数为概率随机切换 NOS。此外，采用失效概率 $f(t)$ 表示系统随时间变化的稳定性。 $f(t)$ 越大，表明系统应对探测攻击时的表现越不稳定，越容易失效。

下面分别模拟非均匀攻击和非重复攻击。前者是专门扫描特定地址段，后者是尽量不重复扫描同一地址段。在仿真实验中，不同策略下的系统失效率 $f(t)$ 变化规律如图 3 和图 4 所示。在这 2 种攻击方式存在的情况下，传统 SDN 架构的系统失效率随时间上升得最快，在 20 个时间单位时，两者的系统失效率分别达到 80% 和 85%，这是因为在 SDN 传统架构中，只有单个 NOS 提供服务，攻击者可以持续不断地对同一目标进行探测直至成功破坏该 NOS，从而达到攻破系统的目的。而在随机切换调度和本文所提调度方法的情景下，系统的失效率上升速度慢，而且随着时间变化，本文所提算法比随机切换调度效果明显，在 100 个时间单位时，非均匀攻击时随机切换调度和本文算法调度下系统失效率分别为 55% 和 30%，非重复攻击时随机切换调度和本文算法调度下系统失效率分别为 56% 和 27%。

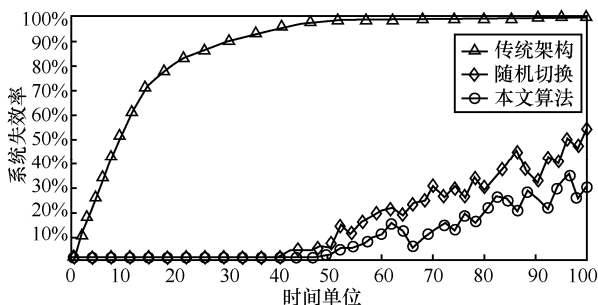


图 3 非均匀攻击下不同调度策略的系统失效率

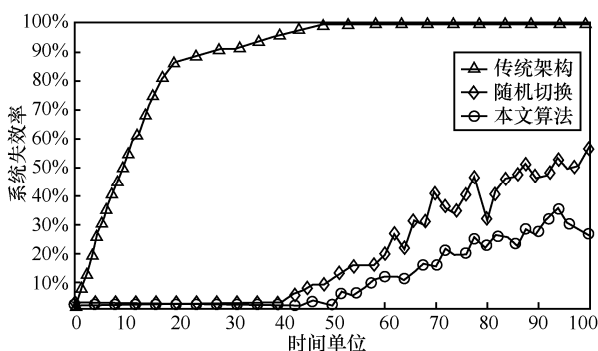


图 4 非重复攻击下不同调度策略的系统失效率

此外，本文分析了系统失效率与 NOS 种类的关系，即 NOS 类的数量对系统稳定性的影响。将 NOS 类的数量设定为 3、5 和 7 进行实验，结果如图 5 所示。表明 NOS 类的数量越多，系统在动态调度的情况下越稳定。因而，可以通过增加 NOS 类的数量加强系统的稳定性。

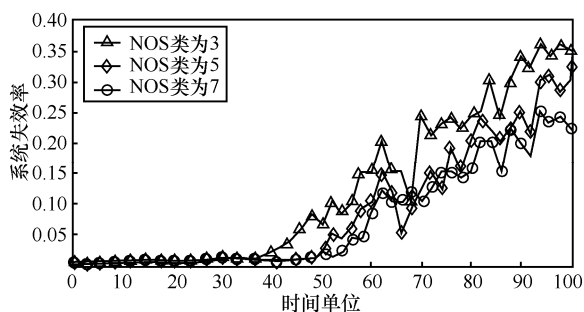


图 5 不同数量 NOS 类的系统失效率

6 结束语

针对无处不在的探测攻击，本文提出了一种基于历史信息的负反馈调度算法，利用假设检验对攻击者的行为进行分析判断，以此为依据进行调度调整，首先对该方法进行了详细的理论分析和仿真实验。实验结果分析表明，相较于现有的 2 种普通的调度算法，静态架构中不切换和以选取系数为概率随机调度，该算法在一定程度上可以增加攻击者的攻击时间成本，因而可以有效防御攻击者的探测攻击。而且，本文还进行了对比实验，发现在同一系统中，SDN 控制器的种类越多，系统表现得越稳定，越不容易被攻击者攻破。

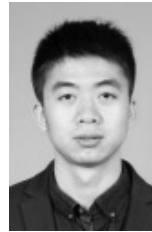
参考文献:

- [1] 全青, 张铮, 邬江兴. 基于软硬件多样性的主动防御技术[J]. 信息安全学报, 2017, 2(1): 1-12.
TONG Q, ZHANG Z, WU J X. Active defense technology based on hardware and software's diversity[J]. Journal of Cyber Security, 2017, 2(1): 1-12.
- [2] PICEK S, HEMBERG E, O'REILLY U M. If you can't measure it, you can't improve it: moving target defense metrics[C]//The Workshop on Moving Target Defense. 2017: 115-118.
- [3] ADELSBACH A, ALESSANDRI D, CACHIN C, et al. Conceptual model and architecture of MAFTIA[R]. 2003.
- [4] KEWLEY D L, BOUCHARD J F. Darpa information assurance program dynamic defense experiment summary[J]. IEEE Transac-

- tions on Systems, Man, and Cybernetics-Part A: Systems and Humans, 2001, 31(4): 331-336.
- [5] 郭江兴. 网络空间拟态防御研究[J]. 信息安全学报, 2016, 1(4): 1-10.
WU J X. Research on cyber mimic defense[J]. Journal of Cyber Security, 2016, 1(4):1-10.
- [6] DESWARTE Y, BLAIN L, FABRE J C. Intrusion tolerance in distributed computing systems[C]//Intrusion Tolerance in Distributed Computing Systems. 2001:110-121.
- [7] JAJODIA S, GHOSH A K, SWARUP V, et al. Moving target defense: creating asymmetric uncertainty for cyber threats[J]. Springer Ebooks, 2011, 54.
- [8] 郭江兴. 拟态计算与拟态安全防御的原意和愿景[J]. 电信科学, 2014, 30(7):1-7.
WU J X. Meaning and vision of mimic computing and mimic security defense[J]. Telecommunications Science, 2014, 30(7):1-7.
- [9] JAFARIAN J H, AL-SHAER E, DUAN Q. Adversary-aware IP address randomization for proactive agility against sophisticated attackers[C]// Computer Communications. 2015:738-746.
- [10] PORRAS P, SHIN S, YEGNESWARAN V, et al. A security enforcement kernel for OpenFlow networks[C]// The First Workshop on Hot Topics in Software Defined Networks. 2012:121-126.
- [11] CHEUNG S, FONG M, PORRAS P, et al. Securing the software-defined network control layer[C]//The 2015 Network and Distributed System Security Symposium. 2015.
- [12] FERGUSON A D, GUHA A, LIANG C, et al. Participatory networking: an API for application control of SDNs[C]//The ACM SIGCOMM 2013 Conference on SIGCOMM. 2013:327-338.
- [13] SHIN S, SONG Y, LEE T, et al. Rosemary: a robust, secure, and high-performance network operating system[C]//The 2014 ACM SIGSAC Conference on Computer and Communications Security. 2014: 78-89.
- [14] SHIN S, PORRAS P, YEGNESWARAN V, et al. FRESCO: modular composable security services for software defined networks[J]. The Network & Distributed Security Symposium, 2013(2):1-16.
- [15] SHIN S, GU G. Attacking software-defined networks: a first feasibility study [C]// ACM SIGCOMM Workshop on Hot Topics in Software Defined Networking. 2013: 165-166.
- [16] BERDE P, HART J, HART J, et al. ONOS: towards an open, distributed SDN OS[C]// The Workshop on Hot Topics in Software Defined Networking. 2014:1-6.
- [17] LAMPORT L, FISCHER M. Byzantine generals and transaction commit protocols[R]. Computer Science Laboratory Sri International OP, 1982.
- [18] HU H, WANG Z, CHENG G, et al. MNOS: a mimic network operating system for software defined networks[J]. Iet Information Security, 2017, 11(6):345-355.
- [19] QI C, WU J, HU H, et al. An intensive security architecture with multi-controller for SDN[C]// Computer Communications Workshops. 2016: 401-402.
- [20] QI C, WU J, CHENG G, et al. An aware-scheduling security architecture with priority-equal multi-controller for SDN[J]. China Communications, 2017, 14(9):144-154.

- [21] PEARSON K. On the criterion that a given system of deviations from the probable in the case of a correlated system of variables is such that it can be reasonably supposed to have arisen from random sampling[M]//Breakthroughs in Statistics. New York: Springer, 1992: 157-175

[作者简介]



吕迎迎 (1993-), 男, 江西进贤人, 国家数字交换系统工程技术研究中心硕士生, 主要研究方向为网络空间安全和软件定义网络。



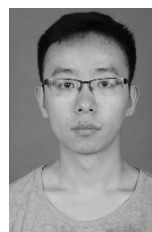
郭云飞 (1963-), 男, 河南郑州人, 国家数字交换系统工程技术研究中心教授、博士生导师, 主要研究方向为网络空间安全、云安全和电信网安全。



王祺鹏 (1993-), 男, 湖北黄冈人, 国家数字交换系统工程技术研究中心硕士生, 主要研究方向为拟态安全防御和网络空间安全。



程国振 (1986-), 男, 山东定陶人, 国家数字交换系统工程技术研究中心助理研究员, 主要研究方向为网络空间安全和软件定义网络。



王亚文 (1990-), 男, 河南郑州人, 国家数字交换系统工程技术研究中心博士生, 主要研究方向为云计算、入侵容忍和网络空间安全。