多样化软件系统量化评估方法

姚远[1,2]，潘传幸[1,2]，张铮[1,2]，张高斐[1,2]
（1. 信息工程大学网络空间安全学院，河南 郑州 450001；
2. 数学工程与先进计算国家重点实验室，河南 郑州 450001）

摘 要：为了指导多样化软件系统在不同应用场景下的冗余变体选取，在研究多样化软件评价指标的基础之上，建立针对软件多样化系统的可用性评价指标体系、安全性评价指标体系、性能指标评价体系，并在此基础上构建了针对多样化软件系统的层次评价体。采用实例验证了所提层次评价体系在小规模变体数目下的可行性。

关键词：拟态防御；多样化软件；量化评估；层次分析
中图分类号：TP309.5
文献标识码：A
doi: 10.11959/j.issn.1000−436x.2020051

Method of quantitative assessment for diversified software system

YAO Yuan[1,2], PAN Chuanxing[1,2], ZHANG Zheng[1,2], ZHANG Gaofei[1,2]
1. Department of Cyberspace Security, Information Engineering University, Zhengzhou 450001, China
2. State Key Laboratory of Mathematical Engineering and Advanced Computing, Zhengzhou 450001, China

Abstract: To instruct the selecting of the redundancy variants for diversified software system at different situations, the evaluation systems of usability, security and performance was constructed by using some diversified software evaluation indicators. Then hierarchical analyzation system (HAS) was introduced based on the three evaluation systems. A real case verify that HAS is practicable at the situation that there are not many variants.

Key words: mimic defense, diversified software, quantitative assessment, analytic hierarchy

1 引言

互联网的高速发展，使计算机软件全球化进程不断向前推进的同时，也带来了软件一元化问题[1-2]。大量相似软件存在于计算机中，容易导致黑客通过利用软件的漏洞，攻击安装了该软件的计算机，从而造成不可估量的经济损失。

安全研究人员意识到软件多样化是应对黑客攻击的一种有效手段。软件多样化是指同一软件的多个实例有不同的二进制执行代码。软件多样化最早应用于容错机制，通过多个可选版本的程序组成多样化冗余系统来获得更高的可靠性和安全性。虽然软件多样化在一定程度上增大了针对软件漏洞攻击与利用的难度，但并没有完全消除恶意威胁。张宇嘉等[3]和庞建民等[4]将软件多样化与拟态防御[5-6]思想相结合，提出了基于软件多样化的拟态防御框架，其框架组成如图 1 所示。该框架不仅对软件采用各种不同的多样化手段，而且引入投票机制，即大数表决机制以产生相较于多版本程序集中单个执行体更加可靠的输出。

基于软件多样化的拟态防御框架中，通常使用多样化编译的方法生成变体集合，包含指令替换、控制流扁平化、代码克隆、动态不透明谓词等各个

收稿日期：2019−12−16；**修回日期**：2020−02−27
通信作者：潘传幸，chuanxing_pan@163.com
基金项目：国家重点研发计划基金资助项目（No.2018YFB0804003）
Foundation Item: The National Key Research and Development Program of China (No.2018YFB0804003)

粒度的混淆手段[7]。分发器将输入分发给各个变体，表决器使用大数表决机制对各个变体的输出进行裁决。该框架有许多优点：扰乱或阻断了攻击链，增加了攻击难度，同时该框架安全风险可控的特点允许软件中存在一定程度的漏洞；框架中多变体的组合应用可以构成相当大的动态空间，用以降低有效利用漏洞和后门进行攻击的风险；冗余使该框架具有内在的可靠性；能够形成共生协同、N 变体、等效多变体。可以看到，为了带来上述优点，该框架将原本一个执行体的工作分发给了一个功能等价的异构（多样化）变体集合，这将会增加性能的损耗。在一些对安全比较敏感的行业（如银行、电网、电子支付等）中，这些性能损耗是可以接受的；但是在一些对用户体验比较敏感的行业（如游戏、社交、多媒体等）中，则要求性能损耗不能太大。目前，对于如何选择 N 个变体使之能构成一个满足各种要求的多样化软件系统，还没有实际有效的测评体系及方法。

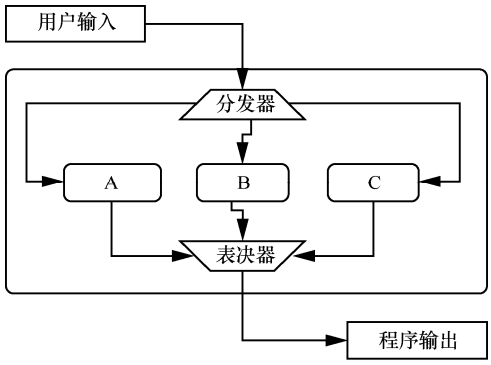


图 1　软件多样化的基于拟态防御框架

本文提出了一种基于层次分析法（AHP, analytic hierarchy process）的多样化软件系统量化评估方法，兼顾选取变体时考虑的主观和客观因素，从而使选出的变体是各方面要求的折中，也为多样化软件系统提供可定制服务贡献了思路。

2　层次分析法

层次分析法是将与决策有关的元素分解成目标、准则、方案等层次，在此基础上进行定性和定量分析的决策方法。这种方法的特点是在对复杂决策问题的本质、影响因素及其内在关系等深入研究的基础上，利用较少的定量信息使决策的思维过程数学化，从而为多目标、多准则或无结构特性的复杂决策问题提供简便的决策方案。层次分析法是对难以完全定量的复杂系统做出决策的模型和方法。

层次分析法根据问题的性质和需要达到的总目标，将目标分解为不同的组成因素，并按照因素间的相互关联影响以及隶属关系将因素按不同的层次聚集组合，形成一个多层次的分析结构模型，最终使问题归结为最低层（方案、措施等）相对于最高层（总目标）的相对重要权值的确定或相对优劣次序的排定。层次分析法适用于具有分层交错评价指标的目标系统，而目标值又难于定量描述的决策问题。多样化软件系统质量问题恰好属于这类问题。层次分析法基本步骤为建立层次结构模型，构造成对比较矩阵，计算权向量并进行一致性检验，计算组合权向量并进行组合一致性检验。

3　多样化软件质量的层次分析模型

3.1　评价指标选取原则

形成评价体系需要选择合适的评价指标。本文根据层次分析理论，采用自上而下的方法，逐步分析，逐层分解，最终确定了由二层评价指标构成的多样化软件系统评价体系。在评价指标选取的过程中遵循以下 4 个原则。

1) 针对性。多样化软件系统不同于一般的软件系统，具体表现为异构性、冗余性以及检查点同步裁决。因为传统软件系统并不具备这些特点，所以传统软件量化评估的指标体系往往不涉及多样化软件系统的特有指标[8-9]。这就要求指标的选取要具有针对性。选取指标时既要侧重于多样化软件系统所特有的质量要素，又要兼顾与传统软件所共有的一些质量要素。

2) 客观性。应用于不同领域的软件系统所关注的质量要素不同，选取指标时应注意软件类别及主要用途，评价指标应反映多样化软件系统的本质特征。

3) 可测性。选取的评价指标必须能够量化表示，能够通过经验统计、数学计算、平台测试等方法得到具体数据。这既是层次分析理论的内在要求，也是评价体系具有应用价值的前提条件。

4) 简明性。评价指标要易于被各方理解和接受。评价指标的选取不在于多少，关键在于在评估过程中，指标所发挥的作用有多大。过多的指标不仅会增加结果的复杂性，有时还会影响评估的客观性。

3.2 层次分析模型

多样化软件系统的层次评价体系由可用性指标体系、安全性指标体系和性能指标体系 3 个部分构成。

可用性指标体系由功能等价性与假阳率 2 个指标构成。多样化软件系统的多样性通过多样化编译来保证，这难免会存在一致性问题，功能等价性是用来衡量执行体之间一致性的指标。由于执行体之间存在不一致问题，表决器难免会产生误报，这种现象称为假阳，假阳率是衡量表决器误报的指标。

安全性指标体系由异构性和攻击表面 2 个指标构成。多样化软件系统的安全能力与异构性紧密相关，目前通常通过统计执行体之间的多样性与差异性来估计异构性[10-11]。攻击表面是衡量一个系统安全能力的另一种量化方式[12]。一般来说，攻击表面越小，系统越安全；攻击表面越大，系统面临的危险越大。

性能指标评价体系由时间性能指标和空间性能指标构成。由于多样化软件系统各执行体之间需要同步表决，这种同步表决机制会带来不可避免的性能损耗；另外，多样化软件系统中多执行体冗余执行，相对传统单执行体软件系统来说，额外的内存空间开销也是无法避免的。总之，性能指标评价体系是层次评价体系中不可缺少的一部分。

综合上述讨论，同时根据 3.1 节中的 4 条评价指标选取原则，本文构建的指标评价体系包括 3 个一级指标和 6 个二级指标。3 个一级指标在准则层 B，分别是可用性、安全性、性能，6 个二级指标在准则层 C，分别是功能等价性、假阳率、异构性、攻击表面、时间性能、空间性能。下一步将对指标评价体系中的各指标分配一定的权重，再按权重将各个具体的指标值整合起来，最终得到多样化软件质量的评估结果。为了在评价过程中避免单一指标的片面性造成的结果不可靠，同时更加全面地评价多样化软件系统的质量，本文将选取的指标评价体系转换成如图 2 所示的层次分析模型。

4 应用实例

本文以应用于互联网行业的某 Web 服务器为例来进行具体的多样化软件评价。进一步地，本次评价的目标是从由多样化编译产生的 4 个服务器变体中，选出 3 个变体构成质量最优的 3−余度变体组合。层次指标评价体系示例如图 3 所示。

在评价过程中，各项评价指标的测量和数据的分析均由专业测试者完成。其中，功能等价性的测量如下：对一组变体组合中的各个变体进行 P 次不同输入，人工观察输出结果，得到 Q 次一致输出，那么功能等价性为 $\frac{Q}{P}$。假阳率的测量结果如下：对一组变体组合进行大量输入，记为 Z 次，通过表决器裁决发现 X 次输出异常，通过人工裁决发现 Y 次输出异常，则假阳率为 $\frac{X-Y}{Z}$。针对异构性的测量，

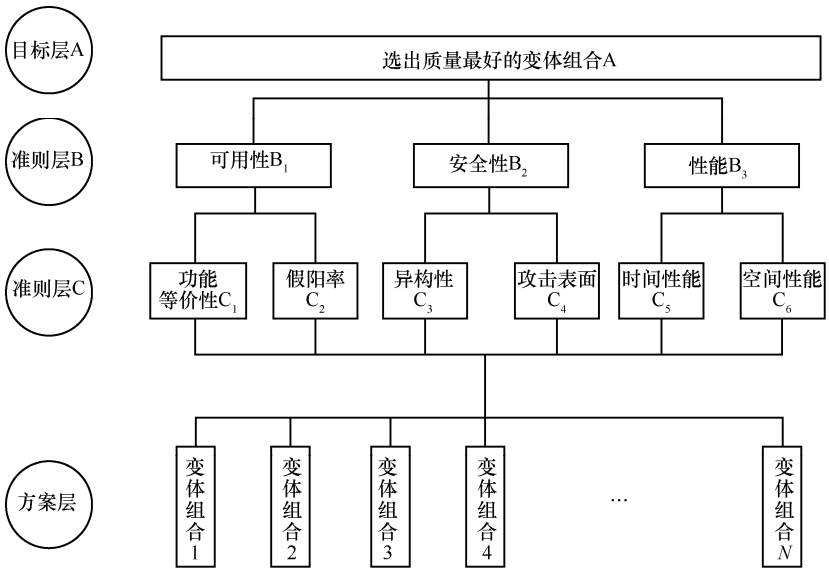


图 2 多样化软件系统的层次分析模型

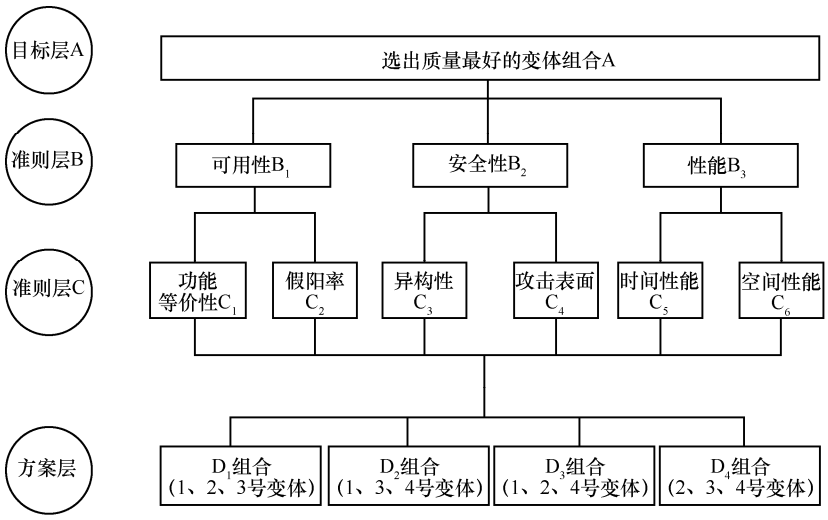


图 3　层次指标评价体系示例

采用张杰鑫等[10]提出的方法，通过计算辛普森多样性指数和差异二次熵，来间接计算变体间的异构性。张铮等[12]将攻击面裁决的概念引入系统表面模型，针对非相似冗余系统进行攻击表面量化。时间性能和空间性能的测量使用基准测试软件完成。

各项指标在准则层的权重设置根据层次排序的结果确定，在方案层的权重由测量结果确定。由于各指标间的测量方式与具体表现形式各异，将测量结果进行等级量化，分为 5 个等级，使用等级量化分数代替测量结果。等级量化分数如表 1 所示。

表 1　　等级量化分数

等级	量化分数
优秀	1.0
良好	0.8
中等	0.6
较差	0.4
非常差	0.2

针对需要评价量化的各个变体组合，同时结合表 1 的量化分数，本文对各变体组合进行定性分析，得出的各变体组合各项指标等级量化得分如表 2 所示。

在评价过程中，使用成对比较矩阵对各指标的重要性进行比较。每个指标的成对比较矩阵 $\boldsymbol{M}$ 中的元素 m_{ij} 表示在下一层第 i 个准则与第 j 个准则的重要程度之比，这个比值根据多样化软件的具体应用领域所重视的质量属性而不同。

针对目标层 A，其矩阵由其下层的可用性 B_1、安全性 B_2、性能 B_3 所决定，再根据 AHP 中常用的 1~9 标度法，可得出成对比较矩阵 $\boldsymbol{M}_{\mathrm{A}}$ =

$$\begin{array}{c} \\ \mathrm{B_1} \\ \mathrm{B_2} \\ \mathrm{B_3} \end{array} \begin{array}{c} \begin{array}{ccc} \mathrm{B_1} & \mathrm{B_2} & \mathrm{B_3} \end{array} \\ \begin{bmatrix} 1 & 1 & 5 \\ 1 & 1 & 6 \\ \frac{1}{2} & \frac{1}{6} & 1 \end{bmatrix} \end{array},$$

因为各个变体组合的可用性和安全性比性能重要，所以 m_{13} 和 m_{23} 的值更大。

同样地，针对准则层 B，可得可用性成对比较矩阵 $\boldsymbol{M}_{\mathrm{B_1}}$、安全性成对比较矩阵 $\boldsymbol{M}_{\mathrm{B_2}}$ 以及性能成对比较矩阵 $\boldsymbol{M}_{\mathrm{B_3}}$ 分别为

表 2　　各变体组合各项指标等级量化得分

变体组合	功能等价性	假阳率	异构性	攻击表面	时间性能	空间性能
D_1 组合	1.0	0.8	0.6	0.4	0.6	0.4
D_2 组合	0.8	0.6	0.8	0.6	0.8	0.6
D_3 组合	0.6	0.4	0.8	0.6	0.6	0.4
D_4 组合	0.6	0.6	0.8	0.8	0.8	0.4

$$\boldsymbol{M}_{\mathrm{B}_1}=\begin{array}{c} \\ \mathrm{C}_1 \\ \mathrm{C}_2 \end{array}\begin{array}{c}\begin{array}{cc}\mathrm{C}_1 & \mathrm{C}_2\end{array}\\ \begin{bmatrix}1 & \frac{1}{2}\\ 2 & 1\end{bmatrix}\end{array}$$

$$\boldsymbol{M}_{\mathrm{B}_2}=\begin{array}{c} \\ \mathrm{C}_3 \\ \mathrm{C}_4 \end{array}\begin{array}{c}\begin{array}{cc}\mathrm{C}_3 & \mathrm{C}_4\end{array}\\ \begin{bmatrix}1 & 3\\ \frac{1}{3} & 1\end{bmatrix}\end{array}$$

$$\boldsymbol{M}_{\mathrm{B}_3}=\begin{array}{c} \\ \mathrm{C}_5 \\ \mathrm{C}_6 \end{array}\begin{array}{c}\begin{array}{cc}\mathrm{C}_5 & \mathrm{C}_6\end{array}\\ \begin{bmatrix}1 & 7\\ \frac{1}{7} & 1\end{bmatrix}\end{array}$$

根据准则层 C 下一层，即方案层的值（表 2），可得出功能等价性成对比较矩阵 $\boldsymbol{M}_{\mathrm{C}_1}$、假阳率成对比较矩阵 $\boldsymbol{M}_{\mathrm{C}_2}$、异构性成对比较矩阵 $\boldsymbol{M}_{\mathrm{C}_3}$、攻击表面成对比较矩阵 $\boldsymbol{M}_{\mathrm{C}_4}$、时间性能成对比较矩阵 $\boldsymbol{M}_{\mathrm{C}_5}$、空间性能成对比较矩阵 $\boldsymbol{M}_{\mathrm{C}_6}$ 分别为

$$\boldsymbol{M}_{\mathrm{C}_1}=\begin{array}{c} \\ \mathrm{D}_1 \\ \mathrm{D}_2 \\ \mathrm{D}_3 \\ D_4 \end{array}\begin{array}{c}\begin{array}{cccc}\mathrm{D}_1 & \mathrm{D}_2 & \mathrm{D}_3 & \mathrm{D}_4\end{array}\\ \begin{bmatrix}1 & \frac{5}{4} & \frac{5}{3} & \frac{5}{3}\\ \frac{4}{5} & 1 & \frac{4}{3} & \frac{4}{3}\\ \frac{3}{5} & \frac{3}{4} & 1 & 1\\ \frac{3}{5} & \frac{3}{4} & 1 & 1\end{bmatrix}\end{array}$$

$$\boldsymbol{M}_{\mathrm{C}_2}=\begin{array}{c} \\ \mathrm{D}_1 \\ \mathrm{D}_2 \\ \mathrm{D}_3 \\ D_4 \end{array}\begin{array}{c}\begin{array}{cccc}\mathrm{D}_1 & \mathrm{D}_2 & \mathrm{D}_3 & \mathrm{D}_4\end{array}\\ \begin{bmatrix}1 & \frac{4}{3} & 2 & \frac{4}{3}\\ \frac{3}{4} & 1 & \frac{3}{2} & 1\\ \frac{1}{2} & \frac{2}{3} & 1 & \frac{2}{3}\\ \frac{3}{4} & 1 & \frac{3}{2} & 1\end{bmatrix}\end{array}$$

$$\boldsymbol{M}_{\mathrm{C}_3}=\begin{array}{c} \\ \mathrm{D}_1 \\ \mathrm{D}_2 \\ \mathrm{D}_3 \\ D_4 \end{array}\begin{array}{c}\begin{array}{cccc}\mathrm{D}_1 & \mathrm{D}_2 & \mathrm{D}_3 & \mathrm{D}_4\end{array}\\ \begin{bmatrix}1 & \frac{3}{4} & \frac{3}{4} & \frac{3}{4}\\ \frac{4}{3} & 1 & 1 & 1\\ \frac{4}{3} & 1 & 1 & 1\\ \frac{4}{3} & 1 & 1 & 1\end{bmatrix}\end{array}$$

$$\boldsymbol{M}_{\mathrm{C}_4}=\begin{array}{c} \\ \mathrm{D}_1 \\ \mathrm{D}_2 \\ \mathrm{D}_3 \\ \mathrm{D}_4 \end{array}\begin{array}{c}\begin{array}{cccc}\mathrm{D}_1 & \mathrm{D}_2 & \mathrm{D}_3 & \mathrm{D}_4\end{array}\\ \begin{bmatrix}1 & \frac{2}{3} & \frac{2}{3} & \frac{1}{2}\\ \frac{3}{2} & 1 & 1 & \frac{3}{4}\\ \frac{3}{2} & 1 & 1 & \frac{3}{4}\\ 2 & \frac{4}{3} & \frac{4}{3} & 1\end{bmatrix}\end{array}$$

$$\boldsymbol{M}_{\mathrm{C}_5}=\begin{array}{c} \\ \mathrm{D}_1 \\ \mathrm{D}_2 \\ \mathrm{D}_3 \\ \mathrm{D}_4 \end{array}\begin{array}{c}\begin{array}{cccc}\mathrm{D}_1 & \mathrm{D}_2 & \mathrm{D}_3 & \mathrm{D}_4\end{array}\\ \begin{bmatrix}1 & \frac{3}{4} & 1 & \frac{3}{4}\\ \frac{4}{3} & 1 & \frac{4}{3} & 1\\ 1 & \frac{3}{4} & 1 & \frac{3}{4}\\ \frac{4}{3} & 1 & \frac{4}{3} & 1\end{bmatrix}\end{array}$$

$$\boldsymbol{M}_{\mathrm{C}_6}=\begin{array}{c} \\ \mathrm{D}_1 \\ \mathrm{D}_2 \\ \mathrm{D}_3 \\ \mathrm{D}_4 \end{array}\begin{array}{c}\begin{array}{cccc}\mathrm{D}_1 & \mathrm{D}_2 & \mathrm{D}_3 & \mathrm{D}_4\end{array}\\ \begin{bmatrix}1 & \frac{2}{3} & 1 & 1\\ \frac{3}{2} & 1 & \frac{3}{2} & \frac{3}{2}\\ 1 & \frac{2}{3} & 1 & 1\\ 1 & \frac{2}{3} & 1 & 1\end{bmatrix}\end{array}$$

然后，计算各成对比较矩阵的特征向量并归一化，得到准则层各指标的层次单排序结果如下。

$$\boldsymbol{\omega}_{\mathrm{A}}=(0.444,0.472,0.084)^{\mathrm{T}}$$

$$\boldsymbol{\omega}_{\mathrm{B}_1}=(0.333,0.667)^{\mathrm{T}}$$

$$\boldsymbol{\omega}_{\mathrm{B}_2}=(0.750,0.250)^{\mathrm{T}}$$

$$\boldsymbol{\omega}_{\mathrm{B}_3}=(0.875,0.125)^{\mathrm{T}}$$

$$\boldsymbol{\omega}_{\mathrm{C}_1}=(0.333,0.267,0.200,0.200)^{\mathrm{T}}$$

$$\boldsymbol{\omega}_{\mathrm{C}_2}=(0.333,0.25,0.25,0.167)^{\mathrm{T}}$$

$$\boldsymbol{\omega}_{\mathrm{C}_3}=(0.200,0.267,0.267,0.266)^{\mathrm{T}}$$

$$\boldsymbol{\omega}_{\mathrm{C}_4}=(0.167,0.250,0.250,0.333)^{\mathrm{T}}$$

$$\boldsymbol{\omega}_{\mathrm{C}_5}=(0.223,0.147,0.297,\ 0.223)^{\mathrm{T}}$$

$$\boldsymbol{\omega}_{\mathrm{C}_6}=(0.222,0.333,0.222,0.223)^{\mathrm{T}}$$

层次单排序的结果即为各指标的下级指标权重。比如，$\boldsymbol{\omega}_{\mathrm{B}_2}=(0.750,\ 0.250)^{\mathrm{T}}$ 说明对于安全性而言，异

构性的权重为 0.750，攻击表面的权重为 0.250。

层次总排序的结果为 $\boldsymbol{\omega}_{\text{res}}=(0.257,\ 0.263,\ 0.246,\ 0.234)^{\text{T}}$。变体 D_2 组合的总排序结果最佳，其值为 0.263，可将其视为 4 个变体组合中质量最好的变体，故应选择 D_2 变体组合构成多样化软件系统。

5　结束语

针对目前难以量化分析在不同场景选择不同多样化变体来使多样化软件系统获益最大化的问题，本文基于层次分析法确定影响各个变体的质量指标权重，构建了一种针对多样化软件系统的质量评价体系。该方法能够有效地量化不同变体组合的质量指标，验证了层次分析法在该领域的适用性以及量化的可行性，进一步地将对多样化软件系统的变体组合的选取具有指导性意义。

然而，如果从 M 个变体中选取 N 个进行评价，将会有 C_M^N 种变体组合，当 M 值较大时，可选择的变体组合数目也较大，这将需要大量的性能测量工作。所以本文提出的多样化软件量化评估方法更适用于小规模变体数目的情况。

参考文献：

[1] ZHANG Y, VIN H, ALVISI L, et al. Heterogeneous networking: a new survivability paradigm[C]//The 2001 Workshop on New Security Paradigms. New York: ACM Press, 2001: 33-39.

[2] STAMP M. Risks of monoculture[J]. Communications of the ACM, 2004, 47(3): 120.

[3] 张宇嘉, 庞建民, 张铮, 等. 基于软件多样化的拟态安全防御策略[J]. 计算机科学，2018, 45(2): 215-221.
ZHANG Y J, PANG J M, ZHANG Z, WU J X. A mimic security defence strategy based on software diversity[J]. Computer Science, 2018, 45(2): 215-221.

[4] 庞建民, 张宇嘉, 邬江兴, 等. 拟态防御技术结合软件多样化在软件安全产业中的应用[J]. 中国工程科学, 2016, 18(6): 74-78.
PANG J M, ZHANG Y J, WU J X, et al. Applying a combination of mimic defense and software diversity in the software security industry[J]. Strategic Study of Chinese Academy of Engineering, 2016, 18(6): 74-78.

[5] 邬江兴. 网络空间拟态防御原理: 广义鲁棒控制与内生安全（上册）[M]. 北京: 科学出版社, 2018.
WU J X. Principles of mimic defense in cyberspace: generalized robust control and endogenous security (Volume 1)[M]. Beijing: Science Press, 2018.

[6] 邬江兴. 网络空间拟态防御原理: 广义鲁棒控制与内生安全（下册）[M]. 北京: 科学出版社, 2018.
WU J X. Principles of mimic defense in cyberspace: generalized robust control and endogenous security (Volume 2)[M]. Beijing: Science Press, 2018.

[7] 张宇嘉, 张啸川, 庞建民. 代码混淆技术研究综述[J]. 信息工程大学学报, 2017, 18(5): 635-640.
ZHANG Y J, ZHANG X C, PANG J M. Survey on code obfuscation research[J]. Journal of Information Engineering University, 2017, 18(5): 635-640.

[8] 张玉凤, 楼芳, 张历. 面向软件攻击面的 Web 应用安全评估模型研究[J]. 计算机工程与科学, 2016, 38(1): 73-77.
ZHANG Y F, LOU F, ZHANG L. Security assessment of Web applications based on software attack surface[J]. Computer Engineering & Science, 2016, 38(1): 73-77.

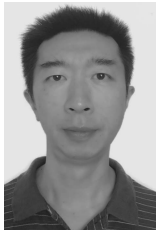
[9] 熊鹏程, 范玉顺. 基于模糊层次分析法的集成软件质量评估模型[J]. 计算机应用, 2006, 26(7): 1497-1499.
XIONG P C, FAN Y S. Integrated software quality evaluation model based on fuzzy analytic hierarchy process[J]. Journal of Computer Applications, 2006, 26(7): 1497-1499.

[10] 张杰鑫, 庞建民, 张铮, 等. 基于非相似余度架构的网络空间安全系统异构性量化方法[J]. 电子与信息学报, 2019, 41(7): 1594-1600.
ZHANG J X, PANG J M, ZHANG Z, et al. Heterogeneity quantization method of cyberspace security system based on dissimilar redundancy structure[J]. Journal of Electronics and Information Technology, 2019, 41(7): 1594-1600.

[11] RAO C R. Diversity and dissimilarity coefficients: a unified approach[J]. Theoretical Population Biology, 1982, 21(1): 24-43.

[12] 张铮, 王立群, 李卫超. 面向非相似余度信息系统的攻击面模型[J]. 通信学报, 2018, 39(S2): 223-230.
ZHANG Z, WANG L Q, LI W C. Research on formal model for an information system’s attack surface with dissimilar redundant architecture[J]. Journal on Communications, 2018, 39(S2): 223-230.

[作者简介]



姚远（1972− ），男，湖北武汉人，博士，信息工程大学教授、博士生导师，主要研究方向为先进编译、并行处理。

潘传幸（1996− ），男，山东梁山人，信息工程大学硕士生，主要研究方向为主动防御。

张铮（1976− ），男，湖北黄冈人，信息工程大学副教授、硕士生导师，主要研究方向为网络空间安全、先进计算。

张高斐（1996− ），男，河南许昌人，信息工程大学硕士生，主要研究方向为主动防御。