专题：内生安全

生物免疫启发下的一种内生安全技术框架

李玉峰[1,2]，曹晨红[1,2]，李江涛[1,2]，王鹏[2,3]
（1. 上海大学，上海 200444；2. 网络通信与安全紫金山实验室，江苏 南京 211100；
3. 中原工学院，河南 郑州 451191）

摘　要：内生安全是网络安全领域的新兴概念与技术方向。受生物免疫机制体现出的内生性安全效应启发，提出了一种内生安全技术框架，剖析了该框架的主要技术挑战，给出了对应的解决方案，分析了该框架的应用场景。分析发现，该框架具有较高的鲁棒性、自主性和自适应性，且具有很强的实用性。

关键词：内生安全；免疫系统；DHR 构造
中图分类号：TP393
文献标识码：A
doi: 10.11959/j.issn.1000−0801.2021051

An endogenous safety and security technical framework inspired by biological immune system

LI Yufeng[1,2]，CAO Chenhong[1,2]，LI Jiangtao[1,2]，WANG Peng[2,3]
1. School of Computer Engineering and Science, Shanghai University, Shanghai 200444, China
2. Purple Mountain Laboratories, Nanjing 211100, China
3. Zhongyuan University of Technology, Zhengzhou 451191, China

Abstract: Inspired by the endogenous safety and security effect of biological immune mechanism, an endogenous safety and security technology framework was proposed, the main technical challenges of the framework were analyzed, the corresponding solutions were given, and the application scenarios of the framework were analyzed. Comprehensive analysis shows that the framework presents high robustness, autonomy and adaptability, and has strong practicability.

Key words: endogenous safety and security, immune system, DHR structure

1　引言

内生安全，是网络安全领域的新兴概念与技术方向，是我国科学家最早针对网络空间安全现状的哲学性归纳与论述[1]。2016 年，中国互联网安全大会（ISC）上，邬江兴院士发表了内生安全的相关论述[2]，先后出版了关于拟态防御与内生安全的中英文著作[3-4]。该理论体系的内生安全问题被抽象为两类。一类是狭义内生安全问题，特指一个软/硬件系统除预期的设计功能之外，总存在包括副作用、脆弱性、自然失效等因素在内的非期望功能；另一类是广义内生安全问题，专指在狭义内生安全问题之上，还包括对最终用户不可见，或所有未向使用者明确声明或披露过的软/

收稿日期：2021−02−01；修回日期：2021−03−15

硬件隐匿功能，例如前门、后门、陷门等“暗功能”问题。当前，“查漏补缺”、加密认证、沙箱蜜罐等传统防御措施很难有效应对基于内生安全问题的不确定性威胁，为此，该理论体系给出了基于内生性安全机制的网络空间拟态防御概念和技术。

奇安信集团董事长齐向东在2019年北京网络安全大会（BCS2019）指出，面对不断变化的网络威胁，网络安全进化到了“内生安全”时代，信息系统需要不断生长出自适应、自主和自成长的安全能力[5]。他在第六届世界互联网大会企业家高峰论坛上还提出，通过建立“一个中心，五张滤网”的内生安全体系，能极大降低网络攻击风险，从而真正保证业务安全[6]。其中，“一个中心”指的是安全运营中心，“五张滤网”指的是网络、身份、应用、数据和行为五张滤网。

本文从生物免疫机制体现出的内生性安全效应出发，提出了生物免疫启发下的一种内生安全三层防御技术框架，针对框架中第二重防线带来的挑战进行了技术分析，给出了可选择的解决方案，分析了该框架的应用场景。

2 生物免疫机制

生物免疫是一个高度复杂的系统，既有生物个体的免疫机制及系统，还有生物群体的免疫机理与机制，共同实现对各种已知和未知病毒的有效防御。

早期研究中，1994 年 Forrest 等[7]和 Kephart[8]在检测恶意软件方面的开创性工作中强调了生物免疫对计算机安全的启发；参考文献[9-12]提出了使用免疫系统模型检测计算机病毒问题，参考文献[13-14]等利用免疫系统的多层模型进行身份识别和入侵检测。近年来，使用机器学习（ML）技术的网络免疫方法研究成为了一个热点，可以通过 ML 检测某个网络传输模式或数据是否是恶意的[15-16]。正如参考文献[17-18]中总结的一样，以往研究基本都围绕异常检测展开，类似生物免疫系统中区分非我（异常对象）和自我（被监测系统的正常特征属性集合）的检测机制。参考文献[18]还总结了 5 个检测主题，即恶意进程检测、异常检测、入侵检测、扫描和洪水检测以及欺诈检测。恶意进程的检测是在主机级别完成的，而入侵、扫描和洪水的检测更多是在网络上处理的问题。欺诈检测主要分析垃圾邮件和网络钓鱼等问题。

本文着重从系统层面考虑生物个体免疫系统对内生安全的研究启示。维基百科对免疫系统进行了很全面的概述[19]。免疫系统通过分层防御保护生物体免受感染。在“分层防御”模型中，生物以三道防线抵御致病微生物的侵害：第一层物理屏障（如表皮）可以防止病原体，如细菌和病毒进入生物体内。病菌如果突破了第一道防线，那么紧接着第二道防线——先天性免疫系统就会产生迅速但非特异性的免疫反应。先天免疫系统是生来就有的免疫系统，存在于所有的动植物中，又称为非特异性免疫、固有免疫、非专一性防御，包括一系列的细胞及相关机制，可以以非特异性的方式抵御外来感染，也就是说先天免疫系统的细胞会非特异地识别并作用于病原体，是一种快速的、广泛的免疫反应[20]。人类在没有疫苗的时候能够战胜新型病毒，依靠的主要就是非特异性免疫。如果病原体再次成功地逃过第二道防线，脊椎动物体内还有第三层保护，即后天免疫系统[21]，也称为获得性免疫、适应性免疫、特异性免疫、专一性防御，是一种经由与特定病原体接触后，产生能识别并针对特定病原体的特异性免疫反应，疫苗接种背后的原理，就是将一种来自于特定病原体的抗原引入机体，在不引发病理症状的前提下，使机体的免疫系统获得对这种病原体的抵抗能力。最后，需要注意的是，先天免疫系统（非特异性免疫）和后天免疫系统（特

异性免疫系统）是密切合作的，而不是互相排斥的[21]，非特异性免疫是特异性免疫发展的基础，从个体发育来看，当抗原物质入侵机体以后，首先发挥作用的是非特异性免疫，而后产生特异性免疫。

3　生物免疫机制的内生安全启示

生物免疫机制能够让生物在不依赖外体的情况下，依靠本体的三重防线就能应对各种已知和未知的病毒，体现出明显的自主性、鲁棒性，而且通过第二道防线和第三道防线的激活作用和密切合作不断形成新的免疫记忆，使整个免疫系统呈现出典型的自适应性和自成长性。因此，一定意义上可以认为，生物免疫是一种典型的内生安全技术示例。

在脊椎动物免疫机制的启发下，若能建立类似的网络安全技术框架，将有效应对各种已知和未知的网络安全威胁。该框架包括三层防御模型：第一层包括物理隔离等安全手段和加密保护等安全技术，建立类似人类皮肤的第一道防线，阻止未经授权的用户进入网络；第二层建立类似人类的非特异性免疫能力。感知和应对未知的安全威胁（未知漏洞、未知后门、未知陷门等），同时形成第三层防御的基础；第三层建立类似人类的特异性免疫能力，在第二层防线感知到未知安全威胁后，分析给出该威胁的特征并为该威胁添加相应的安全策略，使未知威胁变成已知特征的威胁，让系统在面对同样或类似安全威胁时能够依靠类人的“免疫记忆”，检测出威胁并进行针对性防御。第三层防线的本质是建立针对已知特定威胁的高度专门化的检测策略和防御策略，产生类似专门疫苗的特定病毒防疫效应。实际上，当前的网络防御措施中，如防火墙、入侵检测（IDS）、IPS、防病毒软件、漏洞修补等，其核心机理基本沿循威胁特征感知及防御的思路，首先必须获得攻击来源、攻击特征、攻击途径、攻击行为等先验知识的支撑，然后才能够对网络威胁进行高效的针对性识别和及时防御，因此，从机理上属于“后天获得性免疫”，可以归类为第三层防御手段，其存在的主要问题是自身无法有效抵御基于系统软/硬件未知漏洞和未知后门等未知威胁（例如零日攻击等）。

4　技术挑战与解决方案

4.1　主要技术挑战

综上可以发现，建立类似脊椎动物三层免疫模型的主要挑战就在于第二层防线的建立，换言之，当前网络信息系统缺乏一种系统内生的能够有效感知和应对未知特征网络威胁的非特异性防御能力。正因为此，网络空间很难形成一整套体系化的内生安全防线，常常呈现出一种“亡羊补牢”场景：一种未知的网络威胁往往只能在爆发并造成危害后才会被发现和分析，建立针对该威胁的知识并添加到防御策略中，实现“未知”变“已知”，然后才能针对性防御。

要建立类生物的第二层防线，获得一种系统内生的非特异性的网络防御能力，核心挑战就在于要能感知和防御未知的网络威胁，同时激活第三层防线建立“免疫记忆”。当前，有很多研究能够在不同程度上实现对未知威胁的检测和防御。

有许多研究基于机器学习的方法检测未知攻击[22-24]。由于正常网络流量是时变的，很难准确建模，而且训练多个攻击模型对特征选择也有很高的要求，因此，这类方法虽然在一定程度上能检测未知的入侵行为，但大多面临检测精度不高、误报率较高等问题。

还有很多研究提出了使用蜜罐技术检测分析未知的网络攻击[25]。蜜罐使用具有很大的局限性，蜜罐收集的数据面很窄，而且蜜罐一旦被攻破，反而可以被利用发动其他攻击，因此，很多时候需要与其他安全措施配合使用。

很多研究认为，类似零日攻击等利用新漏洞

或新技术的新型攻击，很难用传统安全方法检测，但包括零日恶意软件在内，很多攻击都会显露出攻击时的一些特殊行为，基于行为分析的未知攻击检测核心是用异常检测查找这些异于常规的行为[26]。但由于不同的攻击通常具有不同的网络行为分布，因此该方法的使用有很大的局限性。

此外，还有一类以动态防御为特征的技术能够抵御未知网络威胁。这类技术通过地址随机化、指令随机化、软件多态化等技术动态改变软/硬件自身或其执行环境，对软/硬件进行防御；或者通过对网络拓扑、网络节点、网络配置或网络业务进行动态化、虚拟化和随机化处理，改变网络静态性、确定性和相似性，有效抵御对目标网络的攻击；或者利用数据随机化技术、*N* 变体数据多样化技术等，动态化改变数据的格式、编码或者表现形式，实现对数据的保护。或者通过可重构技术、基于异构平台的应用热迁移技术、Web 服务多样化等动态化技术，动态改变平台从而使平台及其上的应用环境呈现出不确定性，使攻击者难以进行有效攻击。2011 年，美国国家科学技术委员会提出了移动目标防御概念，该技术的核心思想致力于构建一种动态、异构、不确定的网络空间目标环境增加攻击者的攻击难度，以系统的随机性和不可预测性来对抗网络攻击[27]。参考文献[28]中介绍了动态目标防御的基础，基于软件变化的动态目标防御方法，以及基于网络和软件栈配置的动态目标防御方法等。

综合上述技术分析可以发现，这些技术或者仅能在一定程度上检测并感知未知威胁；或者主要依靠伪装或动态化技术增加攻击难度，从而实现对未知威胁的防御；或者准确性不能确保或实用性受限，很难同时提供高可靠、高可信、高可用一体的对未知威胁的感知和防御能力。

4.2 DHR 构造的内生安全效应

动态异构冗余（dynamic heterogeneous redundancy，DHR）构造，是为应对网络空间中基于未知漏洞、后门等未知威胁，提供一种基于内生安全机理的普适性构造方法[29]。

信息系统传统构造与 DHR 构造的主要差别如图 1 所示，传统构造方法由单一执行体完成确定的系统功能，其特性可以归纳为静态性和单一性，攻击者一旦掌握了该执行体的漏洞或后门，执行体可能就对攻击者单向透明。DHR 构造的特性是动态、异构、冗余。DHR 构造主要包括分发代理、运行执行体集、裁决器、负反馈调度和异构执行体池。其中，分发代理负责将外部的输入信号序列分发给运行执行体集中的各个功能等价

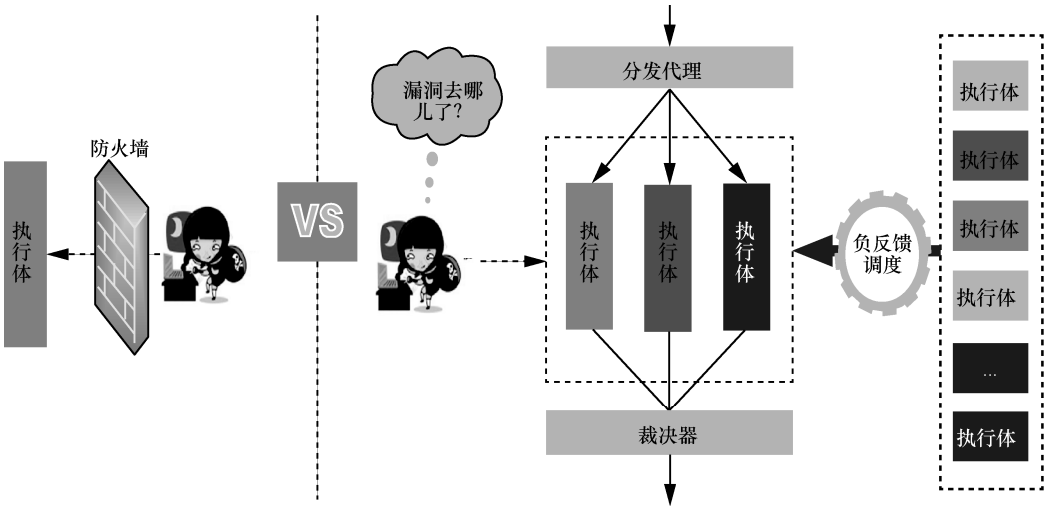

图 1　传统构造与 DHR 构造的主要差别

异构执行体，这些执行体完成处理后将结果矢量输出给裁决器，裁决器对所有执行体产生的输出矢量组成可归一化的裁决界面，然后通过大数裁决、迭代裁决等裁决准则得到最终输出结果。通过裁决若发现了某执行体输出异常，则负反馈调度器根据内部预先设置的调度策略和智能学习算法，激活并下发指令会使相关部件动态完成对该执行体及当前运行环境的更换、迁移、清洗、重组、重构等操作，这一过程是迭代执行的，直至判决器异常情况消失或发生频度低于某个设定的阈值为止。

DHR 构造建立在“相对正确公理”基础之上。该公理可以通俗表述为：“人人都存在这样或那样的缺点，但极少出现独立完成同样任务时，多数人在同一个地点、同一时间、犯完全一样错误的情形”[4]。有研究者将其命名为“相对正确”公理(true relatively axiom，TRA)，也称之为“共识机制”。实际上，成熟的非相似余度架构（dissimilar redundancy structure，DRS）也是相对正确公理的一种实践应用。美国波音公司在开发基于 DRS 架构的飞行控制仪过程中，为确保软/硬件的异构性最大，采用了极为严格的工程管理手段和技术开发方法，通过选拔不同教育背景、技术背景甚至文化背景的人员组成完全独立的多个研发团队，各自使用不同的开发语言和工具，以达到尽力避免或抑制共模故障或失效的目的。这种构造的飞行控制器的失效概率低于 10^{-11}。采用 DRS 架构设计的 F16 战机飞行控制器的失效率也低于 10^{-8}。当然，获得超高可靠性的同时，这种开发模式的代价也是非常高昂的。

DHR 架构集成了 DRS 架构的异构冗余属性，因此同样都是一种超高可靠性架构。需要说明的是，在异构冗余之外，DHR 架构新导入了动态性和随机性，从而新增了抗网络攻击的性能。除了通过共识机制对已经发现的异常执行体进行动态替换之外，DHR 架构还建议不定期地对当前运行的异构执行体集合进行随机变换，或者对异构执行体进行随机重构，又或是借助虚拟化等技术改变运行环境等配置，从而使攻击者很难再次复现以往曾成功的攻击场景。从理论上讲，攻击者只有同时攻击并控制超过一半以上的执行体时，DHR 构造的信息系统才不再具有可信性。显然，系统性能高度取决于异构执行体的数量。更多的异构执行体通常意味着攻击难度的加大和裁决器输出可信性的提高。参考文献[4]的仿真表明，在不同强度的攻击扰动下，3 个异构执行体的 DHR 架构就能极地大增加攻击的难度，使系统取得极高的可信性。因此，DHR 架构也是一种高可信的架构。

综合上述分析可以发现，DHR 构造具有显著的内生安全效应。

（1）对未知威胁的感知和防御能力。在未知攻击无法取得运行执行体多数优势情况下，DHR 架构显然能够借助“相对正确”公理的逻辑表达机制，在不依赖攻击者先验知识或行为特征信息条件下提供高置信度的未知攻击感知功能。而且，通过异构冗余机制确保系统被攻击时仍能保持输出正常，消除未知攻击的影响，因此 DHR 架构能够同时实现对未知威胁的感知和防御，满足上述的第二重防线要求。此外，这种不依赖关于先验知识且不需要在目标对象内部设置任何探针的未知攻击感知手段，可以结合设备的日志和异常数据快照，实现未知漏洞后门发现、恶意攻击代码捕获、攻击者溯源等，最终找到未知攻击的相关特征并形成先验知识，激活第三层防线并形成“免疫记忆”。

（2）功能安全和网络安全一体化保障能力。维基百科中将功能安全（functional safety）称为机能安全，缩写为 FuSa，指的是系统或组成零件在接受输入信号后，可以正常执行动作。目的是避免直接或间接（经由设备或环境）造成人员伤亡、财产损失或环境污染等[30]。通俗意义上说，功能安全指的是任一随机故障、系统故障或共因失效都不会导致安全事故。功能安全一般可以借由平均故障间隔（MTBF）及安全故障失效比率（safe failure fraction，SFF）验证和衡量。维基百科中，

将网络安全（network security）聚焦在黑客通过基于网络的入侵达到窃取敏感信息、造成企业网络无法正常营运等目的，包括设备安全、软件安全和信息安全。本质上讲，功能安全聚焦于系统或组件故障失效带来的风险，网络安全聚焦于人为攻击带来的威胁。如前所述，DHR 架构的异构冗余属性使其能获得高可靠性，能够保障功能安全，在此基础上，动态特性的引入使其能获得高可信性，能够保障网络安全，因此是一种能够提供广义鲁棒控制的创新架构。

5 一种生物免疫启发下的内生安全技术框架简介及应用

5.1 框架简介

本文提出的生物免疫启发下的一种内生安全技术框架如图 2 所示，左侧部分是脊椎动物免疫系统三道防线示意图，右侧是内生安全技术框架对应的三层防御示意图。

该框架的第一层防线类似人类皮肤等物理屏障，对目标信息系统进行隔离、加密等防护；在第二层防线中，本文认为可以通过 DHR 构造等技术使目标信息系统感知和应对各种未知威胁，同时激活第三层防御，通过分析并获得该未知威胁的特征，形成类人的“免疫记忆”，将“未知”威胁变成“已知”。基于先验知识的防火墙、IDS 等各种传统安全设备都可以服务于第三道防线，这些设备可以根据已知的“免疫记忆”快速地对各种威胁进行针对性检测和防御。

该框架的鲁棒性、自主性、自适应和自成长性使其呈现出明显的内生安全效应。一方面该框架有机融合了多重防线的技术优点，使其自主具备了对已知和未知威胁的快速感知与防御能力；另一方面，通过防线间的免疫记忆激活与累加机制，使整个框架的防御能力能够不断地自适应和自成长，能够更及时动态地应对威胁；此外，DHR 构造的异构冗余机制还使框架具备了高可靠性。

5.2 框架应用

网络安全的状况正在经历发展的拐点。安全威胁严重程度与日俱增，安全事件数量呈指数级增长，安全运营团队疲于应对。威胁形势瞬息万变，各种威胁的复杂度越来越高，传统方法已很难有效应对。安全事件的危害越来越大，不仅影响人民的财产安全，还影响到生命安全和国家安全。

这种安全拐点带来的巨大挑战需要现有网络安全防御从理念、体系、架构和技术等全方面进行新的思考、分析、设计与开发。本文受生物免疫机制启发，基于已有技术提出了一种具有内生安全效应的技术框架。该框架能够提供高可靠、高可信与一体的安全效果，且可采用的技术均是已经商业化应用技术或工程化验证技术，因此具有很强的实用性。当然，框架存在一定程度的复杂性，框架的实施也会相应地增加成本。

若目标网络或信息系统要求高可信的网络安

图 2 生物免疫启发下的一种内生安全三层防御技术框架示意图

全保障，例如云的安全防护、重要网络的安全防护等，可以采用该框架。此时，框架第二层防线除了可以选择 DHR 构造技术之外，还可以选择其他的具有未知威胁感知和防御能力的新型技术，例如，动态防御、蜜罐、沙箱、异常检测等技术及这些技术的综合应用。

若目标网络或信息系统要求高可靠、高可信的功能安全与网络安全一体化保障，可以采用该框架。此时，第二层防线目前可选择的技术可能只有 DHR 构造技术。以车联网为例，该网络不同于传统 IT 网络的重要之处就是，它是综合了信息网络和物理环境的多维复杂 CPS（cyber-physical system），其应用环境具有开放性、动态性、多变性、欺骗性等特殊问题，对功能安全、网络安全有更严苛的要求。从功能安全角度方面，要求能够应对复杂场景可能存在的失效甚至失控风险，保障系统在预定义的规范场景内能够正确输出，同时能够容忍超出规范场景的干扰、噪声等；从网络安全角度方面，要求系统能够抵御攻击、保护自身、抗欺骗、反窃取等。车联网中，汽车感知决策部件、车内网络、V2V 和 V2I 的关键安全信息通告、OTA 安全信息更新组件等，既关乎人身安全（safety 领域），又关乎网络攻击（security 领域），是一类“功能安全+网络安全”关键组件。针对这类关键组件，理想的安全解决方案是一体化增强功能安全与网络安全。然而，通常的实际情况却是“此消彼长”，举例来说，为了保障网络安全，很多主机厂将防火墙/IDS 等安全防护系统接入汽车内部通信网络中，但这些系统的设计缺陷可能导致故障，使汽车内部网络中断，从而带来功能安全事故。而 DHR 构造是能够解决此类互斥矛盾，给出功能安全、网络安全一体化保障的新技术。

6　结束语

由于自然界已经为许多现实世界中的问题找到了解决方案，因此，许多研究试图从生物免疫系统机理和机制上寻找网络免疫能力产生的答案。人类对免疫系统的认知存在一个不断深入过程，现今人们正在以“分层防御”的模型理解。

以往借鉴生物免疫的网络安全技术研究，大多聚焦在借鉴区别“自我”与“非我”的免疫机理上，主要应用在异常检测领域中。本文从系统层面的免疫机制出发，探索三层防御模型对网络安全技术的启发。基于近年来在未知威胁感知与防御技术上取得的重要技术突破，提出了一种具有鲁棒性、自主性、自适应和自成长性的内生安全技术框架。这是第一项系统阐述脊椎动物三重防线启发下的具有内生安全效应的网络防御技术框架，虽然还有很多问题需要深入澄清，很多技术需要进一步攻坚，但是，随着对未知威胁感知和防御能力的持续提升，未来的网络将会全面建立起自主免疫系统，释放网络空间的内生安全效应。

参考文献：

[1] 邬江兴.鲁棒控制与内生安全[J]. 网信军民融合, 2018(3): 23-27.
WU J X. Robust control and endogenous safety[J]. Civil-Military Integration on Cyberspace, 2018(3): 23-27.

[2] 科学网. 拟态防御或助网络安全实现再平衡[EB] . 2016.
ScienceNet. Mimic defense may help rebalance network security[EB]. 2016.

[3] 网络空间拟态防御原理——广义鲁棒控制与内生安全（第二版）上册 [M]. 北京: 科学出版社, 2018.
Principles of mimic defense in cyberspace——generalized robust control and endogenous security (second edition) volume One[M]. Beijing: Science Press, 2018.

[4] WU J X. Cyberspace mimic defense - generalized robust control and endogenous security[M]. Switzerland: Springer International Publishing, 2020.

[5] 齐向东. 网络安全已进化到“内生安全”时代 [EB]. 2019.
QI X D. Network security has evolved into the era of “endogenous security”[EB]. 2019.

[6] 齐向东.网络安全形势有三大转变[EB]. 2019.
QI X D. There are three major changes in the cyber security situation[EB]. 2019.

[7] FORREST S, PERELSON A S, ALLEN L, et al. Self-nonself discrimination in a computer[C]//Proceedings of 1994 IEEE computer society symposium on research in security and privacy. Piscataway: IEEE Press, 1994: 202-212.

[8] KEPHART J O. A biologically inspired immune system for computers[C]//Proceedings of the Fourth International Workshop on Synthesis and Simulation of Living Systems, Artificial Life IV: Citeseer. [S.l.:s.n.], 1994.

[9] DASGUPTA D. Artificial immune systems and their applications[M]. Heidelberg Springer Science & Business Media, 2012.

[10] LAMONT G B, MARMELSTEIN R E, VAN VELDHUIZEN D A. A distributedarchitecture for a self-adaptive computer virus immune system[M]//New ideas in optimization. [S.l.:s.n.], 1999: 167-184.

[11] KEPHART J, SORKIN G, SWIMMER M, et al. Blueprint for a computer immune system[C]//Artificial immune systems and their applications. [S.l.:s.n.], 1999: 242-261.

[12] FORREST S, HOFMEYR S A, SOMAYAJI A. Computer immunology[J]. Communications of the ACM, 1997, 40(10): 88-96.

[13] DASGUPTA D. Immunity-based intrusion detection systems: A general frame- work[C]//Proceedings of the 22nd National Information Systems Security Conference. [S.l.: s.n.], 1999: 18-21.

[14] HARMER P K, WILLIAMS P D, GUNSCH G H, et al. An artificial immune system architecture for computer security applications[J]. IEEE transactions on evolutionary computation, 2002, 6(3): 252-280.

[15] MTHUNZI S N, BENKHELIFA E, BOSAKOWSKI T, et al. A bio-inspired approach to cyber security[C]//Proceedings of Machine Learning for Computer and Cyber Security: Principle, Algorithms, and Practices. Boca Raton: CRC Press, 2019:75.

[16] WLODARCZAK P. Cyber immunity[C]//International Conference on Bioinformatics and Biomedical Engineering. Heidelberg: Springer, 2017: 199-208.

[17] RAUF U. A taxonomy of bio-inspired cyber security approaches: existing techniques and future directions[J]. Arabian Journal for Science and Engineering, 2018, 43(12): 6693-6708.

[18] FERNANDES D A, FREIRE M M, FAZENDEIRO P A, et al. Applications of artificial immune systems to computer security: A survey[J]. Journal of Information Security and Applications, 2017, 35: 138-159.

[19] BECK G, HABICHT G S. Immunity and the invertebrates[J]. Scientific American, 1996, 275(5): 60-66.

[20] GENE M. Innate or non-specific immunity[EB]. 2006.

[21] PANCER Z, COOPER M D. The evolution of adaptive immunity[J]. ANNU REV IMMUNOL, 2006(24): 497-518.

[22] MEIRA J, ANDRADE R, PRAÇA I, et al. Performance evaluation of unsupervised techniques in cyber-attack anomaly detection[J]. Journal of Ambient Intelligence and Humanized Computing, 2020, 11(11): 4477-4489.

[23] DUESSEL P, GEHL C, FLEGEL U, et al. Detecting zero-day attacks using context-aware anomaly detection at the application-layer[J]. International Journal of Information Security, 2017, 16(5): 475-490.

[24] SABEEL U, HEYDARI S S, MOHANKA H, et al. Evaluation of deep learning in detecting unknown network attacks[C]// Proceedings of 2019 International Conference on Smart Applications, Communications and Networking (SmartNets). Piscataway: IEEE Press, 2019: 1-6.

[25] MAHAJAN V, PEDDOJU S K. Integration of network intrusion detection systems and honeypot networks for cloud security[C]//Proceedings of 2017 International Conference onComputing, Communication and Automation (ICCCA). Piscataway: IEEE Press, 2017: 829- 834.

[26] YU Y H, YU F, WU X P. Unknown attack detection model based on network behavior analysis[J]. Chinese Journal of Network and Information Security, 2016, 2(6): 54.

[27] MAUGHAN D, NEWHOUSE W D, VAGOUN T. Introducing the federal cyber- security r&d strategic plan[J]. 2012.

[28] 卿昱. 动态目标防御—为应对赛博威胁构建非对称的不确定性[M]. 北京: 国防工业出版社, 2014.
QING Y. Dynamic target defense—constructing asymmetric uncertainty in response to cyber threats[M]. Beijing: National Defense Industry Press, 2014.

[29] 扈红超, 陈福才, 王禛鹏. 拟态防御 DHR 模型若干问题探讨和性能评估[J]. 信息安全学报, 2016, 1(4): 40- 51.
HU H C, CHEN F C, WANG Z P. Discussion on several issues and performance evaluation of mimic defense DHR model[J]. Journal of Cyber Security, 2016, 1(4): 40-51.

[30] 刘建侯. 功能安全技术基础[M]. 北京: 机械工业出版社, 2008.
LIU J H. Fundamentals of functional safety technology[M]. Beijing: Machinery Industry Press, 2008.

[作者简介]

李玉峰（1975− ），男，上海大学教授、博士生导师，主要研究方向为网络信息安全管控、智能系统网络安全、宽带网络等。

曹晨红（1991− ），女，博士，上海大学计算机学院讲师，主要研究方向为网络测量与安全、物联网系统与网络、智能感知技术。

李江涛（1990− ），男，博士，上海大学计算机学院讲师，主要研究方向为公钥密码学、车载网安全与隐私保护。

王鹏（1985− ），男，博士，中原工学院前沿信息技术研究院讲师，主要研究方向为智能系统安全、新型网络与通信安全。