蜜罐技术研究新进展

石乐义* 李 阳 马猛飞

(中国石油大学(华东)计算机与通信工程学院 青岛 266580)

摘 要：蜜罐技术是网络防御中的陷阱技术，它通过吸引诱骗攻击者并记录其攻击行为，从而研究学习敌手的攻击目的和攻击手段，保护真实服务资源。然而，传统蜜罐技术存在着静态配置、固定部署等先天不足，极易被攻击者识别绕过而失去诱骗价值。因此，如何提高蜜罐的动态性与诱骗性成为蜜罐领域的关键问题。该文对近年来国内外蜜罐领域研究成果进行了梳理，首先总结了蜜罐发展历史，随后以蜜罐关键技术为核心，对执行过程、部署方式、反识别思想、博弈理论基础进行了分析；最后，对近年来不同蜜罐防御成果分类叙述，并对蜜罐技术发展趋势进行了分析陈述，针对潜在安全威胁，展望新兴领域防御应用。

关键词：网络安全；蜜罐技术；蜜网；反蜜罐；攻防策略；主动防御

中图分类号：TP393.08 **文献标识码**：A **文章编号**：1009-5896(2019)02-0498-11

DOI: 10.11999/JEIT180292

Latest Research Progress of Honeypot Technology

SHI Leyi LI Yang MA Mengfei

(*College of Computer and Communication of Engineering, China University of Petroleum, Qingdao* 266580, *China*)

Abstract: Honeypot technology is a network trap in cyber defense. It can attract and deceive attackers and record their attack behavior, so as to study the target and attack means of the adversary and protect real service resources. However, because of the static configuration and the fixed deployment in traditional honeypots, it is as easy as a pie for intruders to identify and escape those traps, which makes them meaningless. Therefore, how to improve the dynamic characteristic and the camouflage performance of honeypot becomes a key problem in the field of honeypot. In this paper, the recent research achievements in honeypot are summarized. Firstly, the development history of honeypot in four stages is summed up. Subsequently, by focusing on the key honeypot mechanism, the analysis on process, deployment, counter-recognition and game theory are carried out. Finally, the achievements of honeypot in different aspects are characterized and the development trends of honeypot technology is depicted.

Key words: Network security; Honeypot technology; Honeynet; Anti-honeypot; Attack-defense strategy; Proactive defense

1 引言

自网络诞生以来，攻击威胁事件层出不穷，网络攻防对抗已成为信息时代背景下的无硝烟战争。然而，传统的网络防御技术如防火墙、入侵检测技术等都是一种敌暗我明的被动防御，难以有效应对攻击者随时随地发起的无处不在的攻击和威胁。蜜罐技术[1]的出现改变了这种被动态势，它通过吸引、诱骗攻击者，研究学习攻击者的攻击目的和攻击手段，从而延缓乃至阻止攻击破坏行为的发生，有效保护真实服务资源。蜜罐技术改变了传统防御的被动局面，其具备如下特点：

(1) 误报率为零：蜜罐技术是一个诱骗陷阱，正常用户不会访问到蜜罐系统，因而所有闯入或者误入蜜罐系统的行为都是非正常行为。

(2) 可检测未知威胁：蜜罐可以捕获任何闯入陷阱的行为，包括已知攻击和未知威胁，因而对于先进可持续攻击(Advanced Persistent Threat, APT)、零日攻击等同样有效。

(3) 系统特性伪装：蜜罐技术可改变系统特征，伪装迷惑攻击者，使其无法根据一般系统固定结构发起针对性攻击。

收稿日期：2018-03-28；改回日期：2018-10-30；网络出版：2018-11-09
*通信作者： 石乐义 shileyi@upc.edu.cn
基金项目：国家自然科学基金(61772551)
Foundation Item: The National Natural Science Foundation of China (61772551)

(4) 消耗攻击资源：蜜罐通过高度仿真被保护系统，与入侵者充分交互，从而消耗攻击资源，保护真实资源。

蜜罐本质在于引诱、欺骗，其价值在于被攻击，通过部署吸引敌手攻击的潜在目标，如漏洞主机、价值信息、请求服务等，吸引攻击者并推测攻击意图、攻击手段等信息。然而，传统蜜罐具有配置静态、位置固定等不足，一旦被攻击者发现或绕过，蜜罐将会立即失效。随着近年来反蜜罐技术的兴起，攻击者开始利用反蜜罐技术探测识别蜜罐陷阱，这使得传统蜜罐纷纷失去诱骗作用。可见，传统蜜罐是一种“被动式主动防御”手段。如何提高系统动态可变性与诱骗能力成为近年来蜜罐领域研究热点。本文旨在对蜜罐发展历程、关键技术与理论验证、研究成果进行总结梳理，为安全领域研究人员提供参考。本文贡献如下：(1) 梳理蜜罐发展历程，归纳蜜罐演化升级阶段。(2) 从防护过程、部署、反蜜罐识别与防护、理论基础层面分析蜜罐关键技术。(3) 分类蜜罐研究成果，以自身优化、技术集成、对外功能、攻击类型和应用场景描述蜜罐具体实现。(4) 预测蜜罐发展趋势，分析新技术优势结合，以边缘计算、新硬件革命等新兴领域预测蜜罐应用域。

2　蜜罐发展历程

蜜罐技术总体发展历程可概括为4个阶段：蜜罐概念形成阶段、技术开创初级阶段、蜜罐技术发展阶段、蜜罐应用创新阶段。

(1) 蜜罐概念形成阶段：1989年，蜜罐概念首次出现于黑客小说《The Cuckoo’s Egg》中，通过制造伪机密数据文件引诱攻击者，实现入侵源反向追踪。当时蜜罐仅作为一种新型防御思路，直至1997年，蜜罐仍处于概念形成阶段。

(2) 蜜罐技术初期阶段：1998年，诱骗工具箱(The Deception ToolKit, DTK)开启蜜罐技术发展初期阶段，DTK由安全专家Cohen开发，并给出基于欺骗理论框架与模型，为蜜罐发展提供理论支持。此后，出现了Honeyd, KFSensor等免费开源蜜罐和商业收费蜜罐[2]，迅速成为安全领域内相关学术与产业界的研究热点。

(3) 蜜罐技术发展阶段：1999年，Spitzner提出的蜜网技术改善了初期蜜罐低交互、易识别、功能单一等缺陷，构建多个蜜罐与其它传统防御方案相结合的新型体系结构。利用真实系统环境构建蜜罐，不易被敌手识别。为解决传统蜜网位置局限问题，分布式概念于2003年被引用至蜜罐与蜜网中。同年，新型部署概念蜜场出现，旨在降低维护成本。此后，Kanga分布式蜜网项目实现了多点位置部署，扩大蜜罐覆盖面。此外，Honeywall, HP Feeds, HoneyState, HoneyToken等作为蜜罐通用组件，可依据项目需求选择性部署至上述蜜罐、蜜网、蜜场中。

(4) 蜜罐创新应用阶段：2004年，蜜罐应用开始转向其它领域，如工业控制系统、蓝牙、USB等，如表1所示。除表中所示蜜罐之外，近年来，蜜罐技术亦扩展至更多新兴领域。伴随新型技术领域的出现，新型恶意攻击紧随其后，如勒索病毒、无线网络数据窃取等。为实现系统保护，蜜罐扩展应用于智能手机、无线网络、BYOD自携设备、物联网等方面。

表 1　蜜罐应用性能比对

蜜罐名称	应用领域	仿真精度	数据质量	可嵌入度
SCADA Honeynet	工控系统	一般	较差	较好
Artemisa	IP话音	优秀	优秀	一般
BluePot	蓝牙	较好	一般	较差
Ghost USB honeypot	USB	较好	一般	优秀

蜜罐前3阶段以网络防御体系结构为主要发展方向，由概念转化为技术，实现蜜罐、蜜网、分布式蜜罐、分布式蜜网、蜜场的演化，将部署结构和优化提升作为发展推动力。蜜罐创新应用阶段则根据新兴技术、攻击方式等衍生出新领域下的蜜罐技术，成为网络安全领域内一项重要防护工具。

3　蜜罐关键技术及理论验证

本节以蜜罐关键技术阶段与理论验证为探索基础，从技术出发，分析蜜罐诱捕、监控、处理功能，并且根据蜜罐部署，探索不同部署方式优缺点。为降低蜜罐识别率，针对反蜜罐技术，描述反蜜罐识别思路。为了提供蜜罐技术理论支撑，概述基于博弈论理论基础的蜜罐方案验证。

3.1　蜜罐防护过程

蜜罐防护过程包括诱骗环境构建、入侵行为监控、后期处理措施3个阶段。

(1) 诱骗环境构建：通过构建欺骗性数据、文件等，增加蜜罐环境甜度，引诱攻击者入侵系统，实现攻击交互目的。交互度高低取决于诱骗环境仿真度与真实性，目前主要有模拟环境仿真和真实系统构建方案。

模拟环境仿真方案通过模拟真实系统的重要特征吸引攻击者，具备易部署优势。利用一种或多种开源蜜罐进行模拟仿真，多蜜罐结合方案有利于不同蜜罐的优势集成；将仿真程序与虚拟系统结合构

建蜜罐自定义架构，提高交互度；对硬件利用模拟器实现硬件虚拟化，避免实际硬件破坏。然而，虚拟特性使模拟环境仿真方案存在被识别风险。

真实系统构建方案则采用真实软硬件系统作为运作环境，降低识别率，极大提高了攻击交互度。在软件系统方面，采用真实系统接口[3]、真实主机服务、业务运作系统[4]等，具备较高欺骗性与交互度，但其维护代价较高且受保护资源面临着一定被损害风险。在硬件设备方面，可直接利用真实设备进行攻击信息诱捕，如将物理可穿戴设备作为引诱节点、以手机SIM卡作为蜜卡等，通过构建真实软硬件系统环境提高诱骗度。在低能耗场景下采用真实软硬件设备引诱攻击者具有一定优势，然而对于某些数据交互频繁的业务系统内，存在高能耗、不易部署、维护成本大等缺陷。

(2) 入侵行为监控：在攻击者入侵蜜罐系统后，可利用监视器、特定蜜罐、监控系统等对其交互行为进行监控记录，重点监控流量、端口、内存、接口、权限、漏洞、文件、文件夹等对象，避免攻击造成实际破坏，实现攻击可控性。如模块监控、事件监控[5]、攻击监控、操作监控、活动监控等，上述攻击入侵行为监控中，不同方案的侧重点不同，高交互蜜罐则需更强监控力度。由于监控范围无法全面覆盖，可能导致监控缺失后果，致使攻击者利用监控盲区损害系统，同时，较大监控范围易捕捉更多信息，全方位访问监控成为一种相对安全措施。

(3) 后期处理措施：监控攻击行为所获得数据，可用于数据可视化、流量分类、攻击分析、攻击识别、警报生成、攻击溯源、反向追踪等。具体处理措施为：提取基础数据，以图表方式展示统计数据；分析关联度，提供入侵行为电子证据；分类恶意特征，过滤恶意用户；分析数据包信息，识别潜在安全威胁；利用水平检测识别攻击分类[6]。后期处理措施以分析方式，使防御系统分析收集数据，掌握攻击信息，实现改善系统防御方案的良性循环。

3.2 蜜罐部署方式

按地理位置分类，蜜罐部署方式可分为单点部署和分布式部署。单点部署将蜜罐系统部署于同一区域，如工控系统工业区、无线网络作用域[7]、特定实验场景模拟区[8]等，部署难度小，但作用范围有限，风险感知能力弱。分布式部署则是将蜜罐系统部署于不同地域[9]，利用分布在不同区域的蜜罐收集攻击数据，因此数据收集范围广，实验数据全面，能有效感知总体攻击态势，但部署较困难且维护成本高。

按部署归属度划分，蜜罐部署方式可分为业务范围部署和外部独立部署。前者将蜜罐部署于真实业务系统内，从而提高蜜罐甜度和交互度。但入侵者可以利用蜜罐作为跳板转向攻击真实系统，因而需要严格监控和数据通信隔离。外部独立部署即蜜罐与真实业务系统处于空间隔离状态，降低将蜜罐作为攻击跳板的风险，但诱骗性能较低。

3.3 反蜜罐应对措施

反蜜罐技术作为一种蜜罐识别工具，使攻击者绕过预设陷阱进而攻击真实资源。应对方案重点在于提升系统仿真能力、监控隐蔽能力。具体措施包括：利用更高欺骗性蜜罐如伪蜜罐、动态蜜罐来代替传统蜜罐；结合软件仿真与真实系统，维持业务系统一致性，提升蜜罐仿真度；将监控实施移向系统较低层或实行外部监控，避免敌手嗅探，实现隐蔽监控。

3.4 蜜罐博弈理论分析

目前蜜罐研究多为工程部署，而较少涉及蜜罐基础理论。敌手与蜜罐对抗属于典型的博弈行为，可以将博弈论[10]应用至蜜罐中，通过博弈分析验证，为蜜罐提供理论支撑。利用信令博弈[11]、非合作不完全信息博弈、贝叶斯不完全信息博弈[12]等验证推理蜜罐系统主动性、有效性、约束条件等。

4 蜜罐研究成果分类

4.1 优化自身配置部署的动态蜜罐

传统蜜罐的静态、固定、无感知等缺陷使其易被敌手识别，反蜜罐技术使蜜罐具有较高被识别风险，从而使攻击者绕过蜜罐或以蜜罐作为跳板攻击其它主机资源。因此，蜜罐自身动态性[13]、反识别能力提升，成为蜜罐发展优化方向。

(1) 动态配置蜜罐：Kuwatly等人[14]于2004年提出基于IDS的动态蜜罐设计架构，利用Nmap, P0f和Snort等工具进行主动探测和被动指纹识别，用Honeyd进行网络仿真模拟，并使用一系列高交互蜜罐与网络重定向流量充分交互，将动态蜜罐引擎与上述组件通信，对Honeyd进行配置并产生输出，且为管理员提供可配置接口。Artail等人[15]为保护组织网络而提出一种用以改善IDS的混合蜜罐方案，具备自适应属性[16]，可根据组织网络变化进行相应调整，将大量未使用的IP地址分配给Honeyd集群，据此模拟生产主机网络。Saeedi等人[17]提出对蜜罐进行动态管理并变更配置方法，根据从路由器、防火墙、入侵检测系统以及蜜罐本身所收集信息更改蜜罐自身配置信息，使蜜罐动态适应整个网

络环境，根据不同网络情况自动调整配置，从而达到最佳状态。Fan等人[18]通过动态创建、配置、部署高低交互蜜罐，模拟多种操作系统而形成一种适应性蜜网方案，其核心模块包括决策和重定向两部分，决策引擎用以捕捉特定网络流量，并将其引导至低交互蜜罐Honeyd中，重定向引擎将低交互蜜罐流量重定向至高交互蜜场中。

(2) 动态部署蜜罐：Hecker等人[19]提出动态网络环境下自动化蜜网部署方案，结合被动、主动两种网络流量探测技术监听网络流量并注入新流量，扫描器可决定扫描期间网络流量增量。用户配置存储于数据表内，扫描器据此区分何种情形下创建新蜜网、限制扫描过程带宽、确定目标网络IP范围等等。Fan等人[20]针对当前缺乏多种蜜网部署统一化平台工具的问题，提出多元化虚拟蜜网管理架构。蜜网请求被感应器自动化处理，请求处理器进行语法规范性检查，在验证正确前提下配置引擎将继续对该请求进行处理，若请求条件为模板，则直接向蜜网模板库中调用；若为其它请求，则根据请求内容生成描述，特定转化模块对该描述解释执行生成特定配置，部署工具集据此部署所请求的“私人定制”蜜网。

4.2 与多项技术相结合的新型蜜罐

技术发展为时代带来变革，同时技术创新性对蜜罐产生推动力，通过借鉴不同技术思想、方法，与其它技术结合形成优势互补，如引入兵家作战思想的阵列蜜罐，结合生物保护色与警戒色概念的拟态蜜罐，利用人工智能、大数据等工具提高防护能力的蜜罐等，实验证实创新思想结合或技术优势集成后的系统具有较高的防御性能、诱骗能力。

(1) 创新型蜜罐：借鉴兵家战争思想，石乐义等人[21]提出阵列蜜罐防御模型，采用分布式自选举控制策略和UDP发言人同步机制实现协同控制和同步通信，将蜜罐与真实服务[22]伪随机变换，形成动态变化的阵列陷阱，从而降低攻击者攻击有价值资源概率。受到生物界保护与警戒机制启发，拟态蜜罐方案被提出，包含3种服务类型：服务、蜜罐、伪蜜罐，根据攻击概率选择蜜罐或伪蜜罐部署方案，其中，伪蜜罐用作警戒色吓退攻击者，而蜜罐作为保护色模拟真实服务，从而实现真实服务针对性保护。此外，对拟态蜜罐进行了博弈推理[23]，验证系统有效性。

(2) 多重融合蜜罐：在文献[3]中，Laurén等人利用多接口蜜罐进行恶意软件分析，为最底层系统调用提供双接口，即每个系统服务都可通过一般系统调用编号和保密编号被访问，同时，对入口点进行多元化配置。多元化接口功能将可疑攻击行为与正常系统行为分离，避免接口为攻击者所用。Saadi等人[24]提出一种新架构，使用蜜网、入侵检测技术、防火墙等在云环境下构建多重防护安全系统。对流量进行访问控制操作，阻止恶意流量进入内部。作为系统核心组件，蜜墙将系统划分为3部分：蜜罐区、以太网区、隔离区。其中，蜜罐区由一系列诱敌深入的Sebek, Honeyd组成，进行数据捕获、控制、分析。Sochor等人[25]通过分析对比时下高交互蜜罐研究方法和开源方案，选取最优化方案并组建可应用工具来创建系统，该系统包含Linux Debian和Web server两种高交互蜜罐，其中，Linux Debian包含大量无用数据和MySQL数据库等内容，若攻击者扫描系统，将观测到Windows, Linux和Cisco路由，这些设备由Honeyd模拟仿真；Web server用以响应80端口请求，使用带有漏洞的Web系统进行监控。Mysql数据库将记录存储攻击者登录、命令执行、脚本运行等活动，并将数据可视化呈现。

4.3 面向特定需求的功能蜜罐

近3年，研究者对蜜罐未知功能进行了探索，蜜罐对外功能由单一诱骗目标逐步进化，形成了更多、更复杂的对外功能，如将蜜罐应用于密码模式探究、网络事件监控、未授权数据访问判断、攻击分析等，为安全防护领域提供了更多功能选择。

(1) Web安全：Buda等人[26]针对Web应用[27]程序安全性问题，构建Web应用蜜罐，对数据进行存储，并将数据挖掘算法应用于安全日志分析。

(2) 密码模式：Mun等人[28]通过分析社会工程学，创建蜜罐网站，结合网络钓鱼、移花接木等攻击思想构建攻击场景并实现对用户密码的模式分析与破解。

(3) 网络监控：Vasilomanolakis等人[5]提出一种蜜罐驱动的网络事件监控器，从分布于不同地理位置(欧洲、亚洲、北美)的蜜罐感应器中获取警报数据，使用HTTPS服务接收数据同时利用公钥基础设施(Public Key Infrastructure, PKI)认证感应器。

(4) 电子数据取证：王传极[29]将蜜罐技术用于电子数据取证，构建蜜网拓扑，以TCPdump, SecureCRT和Walleye分别监听网关端口、仿真终端程序及分析远程日志。攻防实验中，攻击方采用X-scan扫描主机漏洞，防御系统记录捕获数据流，分析X-scan扫描类型关联度，针对入侵者的扫描行为提供电子证据。

(5) 非法数据访问：Ulusoy等人[30]提出MapRe-

duce系统中未授权数据访问检测的蜜罐模型，使用数据控制器根据实际数据生成蜜罐数据，并对真实数据和虚假数据进行同步更新。在MapReduce部件获悉蜜罐数据位置信息的前提下，确保已认证部件访问正确真实数据。蜜罐数据遍布整个系统，当攻击者访问这些数据时，将向数据控制器发送警报。

(6) 恶意软件分析：Skrzewski等人[31]对服务器端蜜罐恶意软件监控性能进行了探究，收集恶意软件活动信息需要蜜罐和项目代理，而两者信息都无法完全覆盖，因此需要一种全面性攻击信息视图。通过比对多种蜜罐系统收集信息，得出结论：服务器端蜜罐系统无法作为未知威胁的信息收集源，而客户端蜜罐则可完成此任务。

(7) 蜜罐诱骗研究：Sochor等人[32]分析蜜网拓扑模型、SSH仿真感应器攻击、模拟Windows服务攻击与Web服务攻击，研究网络威胁检测中蜜罐与蜜网吸引力，即蜜罐甜度。实验表明安全防御措施对诱惑攻击者起到重要推动作用。Dahbul等人[33]利用网络服务指纹识别增强蜜罐欺骗能力，构建3种攻击威胁模型来分析指纹识别潜在安全威胁，并在此基础上建立蜜罐系统和真实系统，通过开放和配置必要端口、固定时间戳、配置脚本等手段对蜜罐进行系统性增强。

(8) 攻击分析研究：Sochor等人[34]提出基于Windows仿真蜜罐的攻击分析方案，部署包含6个Dionaea蜜罐的模拟Windows分布式蜜网，进行攻击捕获，统计攻击连接数，分析攻击类型、攻击源地理位置及其所使用操作系统类型，分析结果表明，中度交互蜜罐对自动化攻击方式更具诱惑力，此外，因用户忽视漏洞修补，导致陈旧攻击威胁依然盛行。

4.4 针对特定攻击类型的安全防护蜜罐

针对特定攻击威胁，如APT、勒索病毒、蠕虫病毒、僵尸网络、系统入侵、DoS与DDoS攻击[35]等，研究者亦在蜜罐领域进行了相关探索。

(1) APT攻击：Saud等人[36]使用NIDS和KFSensor蜜罐对APT攻击进行主动检测，当蜜罐服务被请求调用运行时，向控制台发送警报信息。

(2) 带宽攻击：针对带宽攻击，Chamotra等人[37]定义了6种不同蜜罐部署方案，其中，ADSL路由蜜罐用以验证部署方案有效性，该蜜罐是一种低交互蜜罐，在WAN接口上仿真Telnet, SSH, SIP和HTTP服务。

(3) 路由攻击：刘胜利等人[38]提出针对Cisco路由攻击的蜜罐CHoney，该蜜罐基于dynamips模拟器实现硬件平台虚拟化并运行实际Cisco IOS提高伪装性，依据所收集攻击信息，进行敏感操作等级判断，并制定相应报警规则。

(4) 垃圾邮件：针对垃圾邮件，郭军权等人[39]设计了一种结合开放中继和开放代理服务功能的分布式邮件蜜罐，进行不同地域空间部署，保证数据采集全面性，建立多种攻击信息相关数据库，通过大量攻击样本分析影响蜜罐邮件诱骗因素及攻击者行为模式。

(5) 无目标大范围攻击：针对无特定目标大范围攻击，贾召鹏等人[40]提出一种集成多个不同内容管理系统(Content Management System, CMS)应用的蜜罐方案，利用协同控制单元选择合适应用蜜罐对攻击做出合理相应，通过记录、监控流量和文件，获知交互信息、文件操作信息及文件快照，进而实现攻击分析。

(6) 恶意URL及URL重定向：Park等人[41]提出基于虚拟环境的应用客户端蜜罐，由蜜罐代理、Hyperviser、URL爬虫和主服务构成，分析网站恶意代码URL。Akiyama等人[42]针对恶意URL重定向问题开展了研究，探索其演化过程，建立蜜罐监控系统，将系统长期部署于实际网络中追踪URL重定向攻击信息。

(7) 勒索蠕虫：Moore[43]将蜜罐技术应用至勒索蠕虫检测，使用两种服务操控Windows安全日志，建立针对攻击的分等级方案对策：第1级，监控文件夹修改事件，并及时向管理员发送邮件告知；第2级，检测到更多活动时，对攻击软件进行信息推测标识，用户据此断开网络账户连接；第3级，出现更高强度活动时，将关停网络；第4级，关闭服务。

(8) 蠕虫病毒：受“影子蜜罐”启发，文献[4]中，Agrawal等人提出无线网络下“影子蜜网”概念，即受保护系统实例。使用过滤器依照MAC表检查无线网络接入节点，并利用Ettercap, Wireshark, Payload sifting 3种工具实现分阶段联合检测异常数据包。首先利用Ettercap检测丢弃未授权接入请求，若攻击者使用ARP欺骗技术，则继续利用Wireshark通过分析数据流速率判断攻击，最后使用Payload sifting识别并标识蠕虫病毒指纹，转向“影子蜜网”的蜜罐，进行充分交互。

(9) 僵尸网络：Al-Hakbani等人[44]利用节点列表、IP地址欺骗和虚假TCP 3次握手技术等攻破僵尸网络端身份认证，提高蜜罐主机接入僵尸网络的成功率。Chamotra等人[45]利用分布式蜜网捕获数据进行僵尸机检测和僵尸网络追踪，输入位于中央服务器的恶意软件库，库中数据用于重建环境并在

沙盒内运行。在此期间，记录本地API调用序列并编码处理，编码序列作为僵尸机检测输入数据，使用支持向量机分类器标识。利用二进制句法特征对所检测僵尸机实施聚类处理，聚类后的僵尸机群即为某个僵尸网络，使其运行在沙盒中，记录其属性并追踪溯源。

(10) 系统入侵：Olagunju等人[46]创建一种蜜网系统用以实时检测入侵行为[47]，该系统包含4个蜜罐主机、1个中心记录主机和1个任务主机。其中，蜜罐系统由路由器、防火墙和Linux服务器组成，Linux提供了SSH服务以引诱攻击者进行攻击；中心记录主机进行源地址、归属地和时间戳相关入侵信息收集；任务主机用以安装、执行重复性服务。

(11) 未知漏洞攻击：Albashir等人[48]提出在早期阶段检测未知漏洞的蜜网系统，为降低风险，系统结合只允许零日攻击进入蜜网的IDPS技术和防火墙技术，利用监控器监视内部全部活动，并使用蜜网全面捕捉记录攻击活动。Kuze等人[49]利用多蜜罐检测漏洞扫描，将37个蜜罐部署在实际运作网络中收集数据，进而实现数据分析评估，创建一种包含源端口号、目的IP、请求状态码等多重因素的特征向量进行分类处理。Chamotra等人[50]建立蜜罐基线标准来检测0day攻击，其创建过程涉及识别、合法系统活动白名单和蜜罐攻击面建模，密切监控攻击者利用的特定漏洞，结果输出为XML文件并对系统漏洞进行分析评估。

(12) 拒绝服务攻击：Anirudh等人[51]提出针对物联网设备的拒绝服务攻击蜜罐解决方案，利用IDS入侵检测系统处理客户端请求，并通过日志库比对信息，将异常请求隔离并引导至蜜罐，记录异常源信息。表2给出了针对拒绝服务攻击的3种不同蜜罐方案。

表 2　应用蜜罐技术的拒绝服务攻击方案

方案	防护体系	攻击识别方法	保护措施
李硕等人[52]	传统防护与高交互蜜罐	主机负荷检测	暂停数据包转发
Sardana等人[53]	自动响应蜜罐	网络流量标记	重定向可疑流量
Sembiring[54]	物理蜜罐主机与虚拟软件服务	攻击模式分析	隔离攻击源IP

李硕等人[52]设计了一种针对拒绝服务攻击的安全防护方案，通过防火墙、入侵检测和访问控制系统组建传统防护体系，对恶意数据实施阻断，并加入高交互蜜罐系统同时接受外部请求，通过检测蜜罐主机工作负荷判断攻击，防火墙将立即暂停数据包转发，从而保护真实服务器。Sardana等人[53]在拒绝服务攻击网络中建立了一种自动响应蜜罐架构，任何到达路由器且去往服务器的网络流量都将被分析标记为合法或攻击标签，可疑流量包将被重定向至蜜罐服务器，全方位隔离。Sembiring[54]提出用以检测和预防拒绝服务攻击的蜜罐，蜜罐将记录攻击者交互信息，使蜜罐能够实时监测攻击，利用Honeyd-viz图表数据分析攻击模式，从而将攻击源IP隔离。

4.5　实施不同场景应用的立体保护蜜罐

传统蜜罐应用场景具有局限性，现今蜜罐已扩展至多种领域，但新事物应用意味着未知安全漏洞的存在。如表3所示，研究者将重点转移到新兴领域内，扩展蜜罐应用范围。

表 3　蜜罐应用场景及学术研究点

应用场景	研究点
社交网络	恶意行为检测
物联网	IoT攻击途径
自携设备	攻击数字取证
体域网	安全通信通道
无线网络	恶意连接检测
	网络数据分析
工业控制网络	非法请求记录
	工控攻击识别
	威胁事件感知
智能设备	恶意数据捕捉
	恶意软件检测
	诈骗信息分析

(1) 社交网络：以用户作为内容生成源使社交网络成为恶意攻击重点目标，Nisrine[55]利用蜜罐检测社交网络恶意文件，挖掘恶意行为。该蜜罐由正常配置文件和对应处理模块构成，与攻击者充分交互检测恶意用户行为，若检测为恶意，处理模块将收集恶意证据，并进一步提取恶意特征，利用机器学习工具进行数据挖掘实现分类，从而过滤恶意用户。

(2) 物联网：Guarnizo等人在文献[9]中提出一种针对物联网设备的可扩展、高交互蜜罐平台，用以研究攻击途径。利用分布于全球不同地理位置的物联网设备与攻击者充分交互，并以密码形式访问，

采用默认密码和弱口令密码两种方式。存储分析捕捉的流量数据，用以统计TCP连接数、被攻击服务类型、判断连接是否执行攻击脚本等操作。

(3) 自携设备：当前自携设备(Bring Your Own Device, BYOD)盛行，员工可随时随地接入公司网络访问资源，但BYOD技术无法满足网络安全事件爆发前的取证要求，Kebande等人[56]结合蜜罐技术提出一种带有数字取证准备的取证模型，用以捕获、加密、存储潜在数字证据，利用Honeyd蜜罐对攻击日志收集并存储至取证数据库内，对数据包目的地、IP地址、源地址、协议等信息进行分析，识别潜在攻击者并获知潜在安全威胁漏洞。

(4) 体域网：体域网(Body Area Network, BAN)用于传输处理人体数据信息，需确保信息及通信通道安全性，文献[8]中，Leonard等人利用基站，将可穿戴设备作为蜜罐引诱节点，建立高安全性通道和自适应通道，保证伪信息正常通信和真实度，使攻击者无法识别。任何关于伪信息的数据干扰或到达延迟都作为攻击出现标志，将生成警报信息。

(5) 无线网络：针对无线网络下恶意连接和病毒软件，邢文娟[57]设计一种基于Android的手机蜜罐，通过FTP仿真服务检测恶意连接，并判断对外数据是否含有隐私数据，从而对实现恶意病毒软件检测。文献[7]中，Wafi等人提出无线网络中蜜罐安全系统方案，分析网络数据包，若判定为合法则进入生产网络中，否则将被集成为数据流流经MHN(Modern Honey Network)，其数据包被Kippo, Dionaea, Glastopf处理，3种蜜罐监测不同端口，完成特定端口入侵检测、攻击检测等任务。

(6) 工业控制网络：Serbanescu等人[58]开发了一种大规模SCADA蜜网系统，用以捕获、收集工业网络数据，分析工控系统潜在恶意行为。蜜罐可仿真工业协议、模拟特定范围的不同通信协议，任何使用非模拟协议的请求都将被记录。在文献[6]中，Vasilomanolakis等人通过重写协议代码使轻量级蜜罐HosTaGe支持工业控制系统的Modbus, S7, SNMP, SMTP等协议，利用攻击记录模块自动生成协议签名文件，从单协议水平检测、多阶段水平检测和净负荷水平检测3个层面对攻击分类，实现ICS攻击识别。李京京[59]将低交互监控蜜罐SuperPot应用于工业控制系统，实现了基于TCP/UDP的24种工业控制网络协议，并进行了数据统计与可视化处理，实现攻击流量分析。

(7) 智能设备：智能设备的普及为人类带来许多便捷之处，攻击者亦对智能设备发起攻击，Ahmed等人[60]设计了智能手机蜜罐系统，使用硬件性能计数器检测恶意软件并采集信息存储至数据库中，利用K均值聚类算法，采用1维和多维欧氏距离进行分类处理。进一步分析可疑进程，在判定该进程为恶意进程之后，强制关闭，并向用户发送预警信息，告知恶意进程所属分类。电话语音服务与互联网结合技术为网络诈骗提供入手点，网络罪犯可利用电话信道发起攻击。Balduzzi等人[61]提出一种新型移动手机蜜罐MobiPot，利用GSM-VoIP网关模拟移动电话基础设施，使用蜜卡(即手机SIM卡)构建物理设备层，通过IP话音软交换系统模拟个人通信过程，收集诈骗短信和诈骗电话，并将内容信息记录在数据库中，对诈骗信息进行分析。

5 蜜罐发展趋势

蜜罐与攻击者之间的攻防演化将持续升级，在自身技术方面，提高蜜罐甜度、欺骗能力[62]及改善传统架构仍是发展重点，主要有：

(1) 人工智能技术与蜜罐相融合：针对入侵者攻击动机，采用人工智能技术，使蜜罐具备智能交互性，提高蜜罐学习、反识别能力，以此获取更多攻击交互数据有利于防御决策。

(2) 区块链技术与蜜罐相融合：针对分布式蜜罐、分布式蜜网等架构，借鉴区块链分布式、去中心化技术，建立基于P2P架构的私有链或联盟链，使蜜罐自动化运作并保证系统内部数据隐匿性。

(3) 遗传演化计算与蜜罐相融合：针对攻防环境的复杂、变换，蜜罐可充分利用演化计算的高鲁棒性、普适性以适应不同环境下不同问题，使蜜罐具备自适应、自组织、自演化等优势。

在蜜罐应用方面，蜜罐与新技术应用相融合、扩展至新兴领域是一种未来趋势：

(1) 各层次云服务(IaaS, PaaS, SaaS)的普及，为安全人员进行蜜罐研究提供了便利，作为云计算的延伸，边缘计算利用了网络边缘设备，具有极低时延优势。将蜜罐与边缘计算结合，对物联网终端蜜罐设备和传感器进行数据收集处理，并将结果传送至云端服务层，提高即时处理速度和降低服务端负荷。

(2) 目前蜜罐研究主要针对传统网络架构，作为一种新型优势网络架构，SDN(软件定义网络)具有可编程、开放接口等特性，而在一些SDN开源项目中，存在拒绝服务攻击、北向接口协议攻击等行为，因此，蜜罐可应用至SDN，从控制器、接口等方面诱骗攻击者，维护网络安全稳定。

(3) 以硬件软件高度结合为特征的“新硬件时

代”来临，无人驾驶技术、3D打印等新硬件设备成为攻击新靶标，可将轻量级蜜罐与新硬件设备结合，识别探测可疑攻击，拒绝恶意指令执行。

6　总结

本文针对蜜罐及其研究现状进行了总结性工作，分阶段描述了蜜罐的发展历史，并对蜜罐技术执行与理论验证进行了分析。依5种类别对蜜罐近年来研究成果进行分类，叙述蜜罐研究具体实现方案。以网络安全全局趋势来看，蜜罐符合信息技术时代背景，以新型技术、新兴领域及蜜罐技术特征为依据，对蜜罐发展趋势进行了探讨。作为一种主动性防御技术，蜜罐将不断发展更新，也将被安全研究领域更广泛地关注与应用。

参 考 文 献

[1] IRVENE C, FORMBY D, LITCHFIELD S, *et al*. HoneyBot: A honeypot for robotic systems[J]. *Proceedings of the IEEE*, 2018, 106(1): 61–70. doi: 10.1109/JPROC.2017.2748421.

[2] 诸葛建伟, 唐勇, 韩心慧, 等. 蜜罐技术研究与应用进展[J]. 软件学报, 2013, 24(4): 825–842. doi: 10.3724/SP.J.1001.2013.04369.
ZHUGE Jianwei, TANG Yong, HAN Xinhui, *et al*. Honeypot technology research and application[J]. *Journal of Software*, 2013, 24(4): 825–842. doi: 10.3724/SP.J.1001.2013.04369.

[3] LAURÉN S, RAUTI S, and LEPPÄNEN V. An interface diversified honeypot for malware analysis[C]. Proccedings of the 10th European Conference on Software Architecture Workshops, New York, USA, 2016: 1–6. doi: 10.1145/2993412.2993417.

[4] AGRAWAL N and TAPASWI S. Wireless rogue access point detection using shadow honeynet[J]. *Wireless Personal Communications*, 2015, 83(1): 551–570. doi: 10.1007/s11277-015-2408-0.

[5] VASILOMANOLAKIS E, KARUPPAYAH S, KIKIRAS P, *et al*. A honeypot-driven cyber incident monitor: Lessons learned and steps ahead[C]. The 8th International Conference on Security of Information and Networks, Sochi, Russia, 2015: 158–164. doi: 10.1145/2799979.2799999.

[6] VASILOMANOLAKIS E, SRINIVASA S, CORDERO C G, *et al*. Multi-stage attack detection and signature generation with ICS honeypots[C]. IEEE/IFIP Network Operations and Management Symposium, Istanbul, Turkey, 2016: 1227–1232. doi: 10.1109/NOMS.2016.7502992.

[7] WAFI H, FIADE A, HAKIEM N, *et al*. Implementation of a modern security systems honeypot honey network on wireless networks[C]. International Young Engineers Forum, Almada, Portugal, 2017: 91–96. doi: 10.1109/YEF-ECE.2017.7935647.

[8] LEONARD A, CAI H, VENKATASUBRAMANIAN K, *et al*. A honeypot system for wearable networks[C]. IEEE 37th Sarnoff Symposium, Newark, USA, 2016: 199–201. doi: 10.1109/SARNOF.2016.7846755.

[9] GUARNIZO J, TAMBE A, BHUNIA S S, *et al*. SIPHON: Towards scalable high-Interation physical honeypots[C]. The 3rd ACM Workshop on Cyber-Physical System Security, New York, USA, 2017: 57–68. doi: 10.1145/3055186.3055192.

[10] 黄开枝, 洪颖, 罗文宇, 等. 基于演化博弈机制的物理层安全协作方法[J]. 电子与信息学报, 2015, 37(1): 193–199. doi: 10.11999/JEIT140309.
HUANG Kaizhi, HONG Ying, LUO Wenyu, *et al*. A method for physical layer security cooperation based on evolutionary game[J]. *Journal of Electronics & Information Technology*, 2015, 37(1): 193–199. doi: 10.11999/JEIT140309.

[11] 石乐义, 赵俊楠, 李芹, 等. 基于信令博弈的网络诱骗防御策略分析与仿真[J]. 系统仿真学报, 2016, 28(2): 348–353. doi: 10.16182/j.cnki.joss.2016.02.013.
SHI Leyi, ZHAO Junnan, LI Qin, *et al*. Signaling game analysis and simulation on network decoy defense strategies[J]. *Journal of System Simulation*, 2016, 28(2): 348–353. doi: 10.16182/j.cnki.joss.2016.02.013.

[12] LA Q D, QUEK T Q S, LEE J, *et al*. Deceptive attack and defense game in honeypot-enabled networks for the internet of things[J]. *IEEE Internet of Things Journal*, 2016, 3(6): 1025–1035. doi: 10.1109/JIOT.2016.2547994.

[13] 刘江, 张红旗, 杨英杰, 等. 基于主机安全状态迁移模型的动态网络防御有效性评估[J]. 电子与信息学报, 2017, 39(3): 509–517. doi: 10.11999/JEIT160513.
LIU Jiang, ZHANG Hongqi, and YANG Yingjie, *et al*. Effectiveness evaluation of moving network defense based on host security state transition model[J]. *Journal of Electronics & Information Technology*, 2017, 39(3): 509–517. doi: 10.11999/JEIT160513.

[14] KUWATLY I, SRAJ M, AL MASRI Z, *et al*. A dynamic honeypot design for intrusion detection[C]. The IEEE/ACS International Conference on Pervasive Services, Beirut, Lebanon, 2004: 95–104. doi: 10.1109/PERSER.2004.1356776.

[15] ARTAIL H, SAFA H, SRAJ M, *et al*. A hybrid honeypot framework for improving intrusion detection systems in protecting organizational networks[J]. *Computers & Security*, 2006, 25(4): 274–288. doi: 10.1016/j.cose.2006.02.009.

[16] PAUNA A, IACOB A, and BICA I. QRASSH—A self-

adaptive SSH honeypot driven by Q-learning[C]. International Conference on Communications, Bucharest, Romania, 2018, 417–422. doi: 10.1109/ICComm.2018.8484261.

[17] SAEEDI A, KHOTANLOU H, and NASSIRI M. A dynamic approach for honeypot management[J]. *International Journal of Information, Security and Systems Management*, 2012, 1(2): 104–109.

[18] FAN W, FERNÁNDEZ D, and DU Z. Adaptive and flexible virtual honeynet[C]. International Conference on Mobile, Secure and Programmable Networking, Paris, France, 2015: 1–17. doi: 10.1007/978-3-319-25744-0_1.

[19] HECKER C and HAY B. Automated honeynet deployment for dynamic network environment[C]. International Conference on System Sciences, Hawaii, USA, 2013: 4880–4889. doi: 10.1109/HICSS.2013.110.

[20] FAN W, FERNÁNDEZ D, and DU Z. Versatile virtual honeynet management framework[J]. *IET Information Security*, 2016, 11(1): 38–45. doi: 10.1049/iet-ifs.2015.0256.

[21] 石乐义, 李婕, 刘昕, 等. 基于动态阵列蜜罐的协同网络防御策略研究[J]. 通信学报, 2012, 33(11): 159–164. doi: 10.3969/j.issn.1000-436x.2012.11.020.
SHI Leyi, LI Jie, LIU Xin, *et al*. Research on dynamic array honeypot for collaborative network defense strategy[J]. *Journal on Communications*, 2012, 33(11): 159–164. doi: 10.3969/j.issn.1000-436x.2012.11.020.

[22] 石乐义, 姜蓝蓝, 贾春福, 等. 蜜罐诱骗防御机理的博弈理论分析[J]. 电子与信息学报, 2012, 34(6): 1420–1424. doi: 10.3724/SP.J.1146.2011.00929.
SHI Leyi, JIANG Lanlan, JIA Chunfu, *et al*. A game theoretic analysis for the honeypot deceptive mechanism[J]. *Journal of Electronics & Information Technology*, 2012, 34(6): 1420–1424. doi: 10.3724/SP.J.1146.2011.00929.

[23] 石乐义, 姜蓝蓝, 刘昕, 等. 拟态式蜜罐诱骗特性的博弈理论分析[J]. 电子与信息学报, 2013, 35(5): 1063–1068. doi: 10.3724/SP.J.1146.2012.01213.
SHI Leyi, JIANG Lanlan, LIU Xin, *et al*. Game theoretic analysis for the feature of mimicry honeypot[J]. *Journal of Electronics & Information Technology*, 2013, 35(5): 1063–1068. doi: 10.3724/SP.J.1146.2012.01213.

[24] SAADI C and CHAOUI H. Cloud computing security using IDS-AM-Clust, honeyd, honeywall and honeycomb[J]. *Procedia Computer Science*, 2016, 85: 433–442. doi: 10.1016/j.procs.2016.05.189.

[25] SOCHOR T and ZUZCAK M. High-interaction linux honeypot architecture in recent perspective[C]. International Conference on Computer Networks, Brunow, Poland, 2016: 118–131. doi: 10.1007/978-3-319-39207-3_11.

[26] BUDA M and BLUEMKE I. Data mining algorithms in the analysis of security logs from a honeypot system[C]. International Conference on Dependability and Complex Systems, Brunow, Poland, 2016: 63–73. doi: 10.1007/978-3-319-39639-2_6.

[27] JIA Zhaopeng, CUI Xiang, LIU Qixu, *et al*. Micro-Honeypot: Using browser fingerprinting to track attackers[C]. IEEE Third International Conference on Data Science in Cyberspace, Guangzhou, China, 2018: 197–204. doi: 10.1109/DSC.2018.00036.

[28] MUN H J and HAN K H. Blackhole attack: user identity and password seize attack using honeypot[J]. *Journal of Computer Virology and Hacking Techniques*, 2016, 12(3): 185–190. doi: 10.1007/s11416-016-0270-6.

[29] 王传极. 基于蜜罐技术捕获的电子数据的证据效力研究[D]. [硕士论文], 华东政法大学, 2015.
WANG ChuanJi. Research on the evidence validity of data capturing by honeypot[D]. [Master dissertation], East China University of Political Science and Law, 2015.

[30] ULUSOY H, KANTARCIOGLU M, THURAISINGHAM B, *et al*. Honeypot based unauthorized data access detection in MapReduce systems[C]. IEEE International Conference on Intelligence and Security Informatics, Baltimore, USA, 2015: 126–131. doi: 10.1109/ISI.2015.7165951.

[31] SKRZEWSKI M. About the efficiency of malware monitoring via server-side honeypots[C]. International Conference on Computer Networks, Brunow, Poland, 2016: 132–140. doi: 10.1007/978-3-319-39207-3_12.

[32] SOCHOR T and ZUZCAK M. Attractiveness study of honeypots and honeynets in internet threat detection[C]. International Conference on Computer Networks, Brunow, Poland, 2015: 69–81. doi: 10.1007/978-3-319-19419-6_7.

[33] DAHBUL R N, LIM C, and PURNAMA J. Enhancing honeypot deception capability through network service fingerprinting[J]. *Journal of Physics*: *Conference Series*, 2017, 801(1): 1–7. doi: 10.1088/1742-6596/801/1/012057.

[34] SOCHOR T, ZUZCAK M, and BUJOK P. Analysis of attackers against windows emulating honeypots in various types of networks and regions[C]. Eighth International Conference on Ubiquitous and Future Networks, Vienna, Austria, 2016: 863–868. doi: 10.1109/ICUFN.2016.7537159.

[35] 武泽慧, 魏强, 任开磊, 等. 基于OpenFlow交换机洗牌的DDoS攻击动态防御方法[J]. 电子与信息学报, 2017, 39(2): 397–404. doi: 10.11999/JEIT160449.
WU Zehui, WEI Qiang, REN Kailei, *et al*. Dynamic defense for DDoS attack using openflow-based switch shuffling approach[J]. *Journal of Electronics & Information Technology*, 2017, 39(2): 397–404. doi: 10.11999/JEIT160449.

[36] SAUD Z and ISLAM M H. Towards proactive detection of

Advanced Persistent Threat (APT) attacks using honeypots[C]. The 8th International Conference on Security of Information and Networks, Sochi, Russia, 2015: 154–157. doi: 10.1145/2799979.2800042.

[37] CHAMOTRA S, SEHGAL R K, ROR S, *et al*. Honeypot deployment in broadband networks[C]. International Conference on Information Systems Security, Jaipur, India, 2016: 479–488. doi: 10.1007/978-3-319-49806-5_27.

[38] 刘胜利, 彭飞, 武东英, 等. CHoney: 一个面向 Cisco 路由器攻击捕获的新型蜜罐[J]. 北京邮电大学学报, 2015, 38(5): 47–53. doi: 10.13190/j.jbupt.2015.05.008.
LIU Shengli, PENG Fei, WU Dongying, *et al*. CHoney: A new honeypot for capturing attacks against cisco routers[J]. *Journal of Beijing University of Posts and Telecommunications*, 2015, 38(5): 47–53. doi: 10.13190/j.jbupt.2015.05.008.

[39] 郭军权, 诸葛建伟, 孙东红, 等. Spampot: 基于分布式蜜罐的垃圾邮件捕获系统[J]. 计算机研究与发展, 2014, 51(5): 1071–1080. doi: 10.7544/issn1000-1239.2014.20120738.
GUO Junquan, ZHUGE Jianwei, SUN Donghong, *et al*. Spampot: A spam capture system based on distributed honeypot[J]. *Journal of Computer Research and Development*, 2014, 51(5): 1071–1080. doi: 10.7544/issn1000-1239.2014.20120738.

[40] 贾召鹏, 方滨兴, 崔翔, 等. ArkHoney: 基于协同机制的Web蜜罐[J]. 计算机学报, 2018, 41(2): 413–425. doi: 10.11897/SP.J.1016.2018.00413.
JIA Zhaopeng, FANG Binxing, CUI Xiang, *et al*. ArkHoney: A web honeypot based on collaborative mechanisms[J]. *Chinese journal of Computers*, 2018, 41(2): 413–425. doi: 10.11897/SP.J.1016.2018.00413.

[41] PARK J H, CHOI J W, and SONG J S. How to design practical client honeypots based on virtual environment[C]. Asia Joint Conference on Information Security, Fukuoka, Japan, 2016: 67–73. doi: 10.1109/AsiaJCIS.2016.19.

[42] AKIYAMA M, YAGI T, YADA T, *et al*. Analyzing the ecosystem of malicious URL redirection through longitudinal observation from honeypots[J]. *Computers & Security*, 2017, 69(1): 155–173. doi: 10.1016/j.cose.2017.01.003.

[43] MOORE C. Detecting ransomware with honeypot techniques[C]. Cybersecurity and Cyberforensics Conference, Amman, Jordan, 2016: 77–81. doi: 10.1109/CCC.2016.14.

[44] AL-HAKBANI M M and DAHSHAN M H. Avoiding honeypot detection in peer-to-peer botnets[C]. IEEE International Conference on Engineering and Technology, Coimbatore, India, 2015: 1–7. doi: 10.1109/ICETECH.2015.7275017.

[45] CHAMOTRA S, SEHGAL R K, and ROR S. Bot detection and botnet tracking in honeynet context[C]. Conference on Information and Communication Technology for Intelligent Systems, Ahmedabad, India, 2016: 563–574. doi: 10.1007/978-3-319-30933-0_56.

[46] OLAGUNJU A O and SAMU F. In search of effective honeypot and honeynet systems for real-time intrusion detection and prevention[C]. The 5th Annual Conference on Research in Information Technology, Boston, USA, 2016: 41–46. doi: 10.1145/2978178.2978184.

[47] MUHAMMET B and RESUL D. A novel honeypot based security approach for real-time intrusion detection and prevention systems[J]. *Journal of Information Security and Applications*, 2018, 41: 103. doi: 10.1016/j.jisa.2018.06.004.

[48] ALBASHIR A A A N. Detecting unknown vulnerabilities using honeynet[C]. First International Conference on Anti-Cybercrime, Riyadh, Saudi Arabia, 2015: 1–4. doi: 10.1109/Anti-Cybercrime.2015.7351929.

[49] KUZE N, ISHIKURA S, YAGI T, *et al*. Detection of vulnerability scanning using features of collective accesses based on information collected from multiple honeypots[C]. Network Operations and Management Symposium, Istanbul, Turkey, 2016: 1067–1072. doi: 10.1109/NOMS.2016.7502962.

[50] CHAMOTRA S, SEHGAL R K, and MISRA R S. Honeypot baselining for zero day attack detection[J]. *International Journal of Information Security and Privacy*, 2017, 11(3): 63–74. doi: 10.4018/IJISP.2017070106.

[51] ANIRUDH M, THILEEBAN S A, and NALLATHAMBI D J. Use of honeypots for mitigating DoS attacks targeted on IoT networks[C]. International Conference on Computer, Communication and Signal Processing, Chennai, India, 2017: 1–4. doi: 10.1109/ICCCSP.2017.7944057.

[52] 李硕, 张权. 基于蜜罐的CC攻击防护体系[J]. 信息安全与通信保密, 2015(9): 99–102. doi: 10.3969/j.issn.1009-8054.2015.09.030.
LI Shuo and ZHANG Quan. Protection system of CC attack based on honeypot[J]. *Information Security and Communications Privacy*, 2015(9): 99–102. doi: 10.3969/j.issn.1009-8054.2015.09.030.

[53] SARDANA A and JOSHI R. An auto-responsive honeypot architecture for dynamic resource allocation and QoS adaptation in DDoS attacked networks[J]. *Computer Communications*, 2009, 32(12): 1384–1399. doi: 10.1016/j.comcom.2009.03.005.

[54] SEMBIRING I. Implementation of honeypot to detect and prevent distributed denial of service attack[C]. International Conference on Information Technology, Computer, and Electrical Engineering, Semarang, Indonesia, 2016: 345–350. doi: 10.1109/ICITACEE.2016.7892469.

[55] NISRINE M. A security approach for social networks based

on honeypots[C]. IEEE International Colloquium on Information Science and Technology, Tangier, Morocco, 2016: 638–643. doi: 10.1109/CIST.2016.7804964.

[56] KEBANDE V R, KARIE N M, and VENTER H S. A generic digital forensic readiness model for BYOD using honeypot technology[C]. IST-Africa Week Conference, Durban, South Africa, 2016: 1–12. doi: 10.1109/ISTAFRICA.2016.7530590.

[57] 邢文娟. 基于Android的手机蜜罐研究与设计[D]. [硕士论文], 中国石油大学(华东), 2016.
XING Wenjuan. The rsearch and dsign of mbile phone honeypot based on android[D]. [Master dissertation], China University of Petroleum (East China), 2016.

[58] SERBANESCU A V, OBERMEIER S, and YU D Y. A scalable honeynet architecture for industrial control systems[C]. International Conference on E-Business and Telecommunications, Colmar, France, 2015: 179–200. doi: 10.1007/978-3-319-30222-5_9.

[59] 李京京. 基于蜜罐技术的ICS威胁感知平台设计与实现[D]. [硕士论文], 郑州大学, 2017.
LI Jingjing. Design and implementation of ICS threat perception platform based on honeypot[D]. [Master dissertation], Zhengzhou University, 2017.

[60] AHMED H M, HASSAN N F, and FAHAD A A. Designing a smartphone honeypot system using performance counters[J]. *Karbala International Journal of Modern Science*, 2017, 3(1): 46–52. doi: 10.1016/j.kijoms.2017.02.004.

[61] BALDUZZI M, GUPTA P, GU L, *et al*. Mobipot: Understanding mobile telephony threats with honeycards[C]. The 11th ACM on Asia Conference on Computer and Communications Security, Xi'an, China, 2016: 723–734. doi: 10.1145/2897845.2897890.

[62] 贾召鹏, 方滨兴, 刘潮歌, 等. 网络欺骗技术综述[J]. 通信学报, 2018, 38(12): 128–143. doi: 10.11959/j.issn.1000-436x.2017281.
JIA Zhaopeng, FANG Binxing, LIU Chaoge, *et al*. Survey on cyber deception[J]. *Journal on Communications*, 2018, 38(12): 128–143. doi: 10.11959/j.issn.1000-436x.2017281.

石乐义：男，1975年生，博士，教授，研究方向为网络安全、博弈理论、移动互联网.

李 阳：女，1993年生，硕士生，研究方向为网络安全、蜜罐、区块链.

马猛飞：男，1993年生，硕士生，研究方向为网络安全、主动防御.