

工业互联网蜜网技术综述

陈曦^{1,2}, 姜亚光³, 林昕³, 周文⁴

(1. 北京大学软件与微电子学院, 北京 100871; 2. 中国电子信息产业发展研究院, 北京 100048;

3. 中国软件评测中心(工业和信息化部软件与集成电路促进中心), 北京 100048;

4. 中国民用航空局民航智慧能源工程技术研究中心, 北京 100088)

摘要: 工业互联网将互联网和物联网技术应用于传统工业领域, 通过连接、监控和优化工业系统中的设备、机器和流程, 实现生产效率的提升、资源利用的优化以及产品和服务的创新。然而, 工业互联网中的复杂设备和协议容易存在安全漏洞, 导致潜在诸多的安全威胁。蜜网是功能强大的网络安全手段, 通过虚拟或模拟的系统、服务或资源, 诱导攻击者进行攻击。一旦攻击者与蜜网互动, 即可监控并记录攻击活动, 有助于提前发现新型网络安全威胁, 改进网络安全防御, 并为安全研究提供数据。通过汇总大量工业互联网蜜网的相关文献和资料, 总结了工业互联网蜜网的基本概念和发展过程, 并介绍了工业互联网蜜网的关键技术, 对设备仿真、协议模拟和部署分析进行了详细的技术介绍。此外, 还针对工业互联网蜜网的功能和结构, 提出了基于ATT&CK (adversarial tactics, techniques & common knowledge) 的企业矩阵模型的蜜网评估体系, 对几种工业互联网蜜网进行了评估, 并对工业互联网未来的研究进行了展望。

关键词: 工业互联网; 蜜网; 蜜罐; 网络安全

中图分类号: TP309.2

文献标志码: A

DOI: 10.11959/j.issn2096-109x.2024064

Overview on industrial Internet honeynet technology

CHEN Xi^{1,2}, JIANG Yaguang³, LIN Xin³, ZHOU Wen⁴

1. School of Software and Microelectronics, Peking University, Beijing 100871, China

2. China Center for Information Industry Development, Beijing 100048, China

3. China Software Testing Center(CSIP), Beijing 100048, China

4. Engineering Research Center of Smart Energy, Civil Aviation Administration of China, Beijing 100088, China

Abstract: The industrial Internet was integrated with Internet and IoT technologies into traditional industrial sectors, with the aim of enhancing production efficiency, optimizing resource utilization, and fostering innovation in products and services. However, the complexity of industrial Internet devices and protocols posed security vulnerabilities, resulting in numerous security threats. Honeynets emerged as a powerful cybersecurity measure, employing virtual or simulated systems, services, or resources to lure attackers. Upon interaction with the honeynet, monitoring and recording of attack activities were conducted, which aided in the early detection of novel

收稿日期: 2023-12-14; 修回日期: 2024-04-14

通信作者: 林昕, linxin@cstc.org.cn

引用格式: 陈曦, 姜亚光, 林昕, 等. 工业互联网蜜网技术综述[J]. 网络与信息安全学报, 2024, 10(5): 23-38.

Citation Format: CHEN X, JIANG Y G, LIN X, et al. Overview on industrial Internet honeynet technology[J]. Chinese Journal of Network and Information Security, 2024, 10(5): 23-38.

cybersecurity threats, enhanced network security defenses, and contributed valuable data for security research. A substantial body of literature and resources on industrial Internet honeynets were synthesized, outlining their fundamental concepts and developmental processes. Key technologies of industrial Internet honeynets, including device simulation, protocol emulation, and deployment analysis, were comprehensively discussed. Additionally, a honeynet assessment system based on the Adversarial Tactics, Techniques & Common Knowledge (ATT&CK) framework was proposed, tailored to the functionalities and structures of industrial Internet honeynets. Several industrial Internet honeynets were evaluated using this model, and the conclusion was addressed with prospects for future research in industrial Internet honeynets.

Keywords: industrial Internet, honeynet, honeypot, network security

0 引言

蜜网是复杂的诱捕网络,通过资源模拟来构建诱捕环境,吸引攻击者并获取其数据,进而分析攻击信息和手段。当攻击者与蜜网交互后,对采集到的数据和日志进行分析。蜜网不仅能获取危险信息,还能转移攻击者的注意力,降低真实资源的安全风险。

近年来,工业互联网安全形势严峻,各类工业互联网攻击事件层出不穷。2010年,美国政府主导的震网蠕虫攻击事件浮出水面^[1],引发了国际主流安全厂商(如卡巴斯基、赛门铁克、安天等)、众多安全研究者(如Langne等)以及多国应急组织和研究机构的全面关注。2013年,一个名为Havex^[2]工业控制系统(industrial control system, ICS)的病毒被发现,其主要的攻击对象是在欧洲使用和开发工业应用程序与机械设备的公司,并成功入侵1 000多家欧洲和北美的能源公司。2014年年初,Havex^[2]开始对工控系统发起攻击,感染数据采集与监视控制(supervisory control and data acquisition, SCADA)系统和工控系统中使用的工业控制软件,其主要目的是窃取工控数据情报。2007年,著名黑客Cr4sh以700美元价格卖出自己开发的黑客工具BlackEnergy,随着开发者对BlackEnergy的不断改进^[3],它逐渐由最初的分布式拒绝服务(distributed denial of service, DDoS)攻击工具变成了可安装各种功能插件的平台。2015年,BlackEnergy还被应用于对乌克兰电力系统的攻击中。2023年,英国电子电气公司豪利士遭到网络攻击,造成经济损失。调查显示,该事件是公司位于全球的多个信息技术系统和数据遭到未经授权访问导致的。由此可见,当前工业互联网安全形势不容乐观。

相对防火墙、网络流量分析等被动防御方法,

蜜网有着攻击者诱捕、早期攻击检测和降低误报率等优势。因此,蜜网已经成为当下不可或缺的防御手段之一,特别是在工业互联网领域,蜜网复杂的网络能够满足工业互联网的多种需求。

1 工业互联网蜜网基本概念

工业互联网蜜网是网络安全手段,为挖掘当前工业互联网中的潜在威胁,通过模拟工业互联网环境中的系统、服务或资源,获取攻击者的信息并进行分析。

1.1 工业互联网蜜网概述

1.1.1 工业互联网安全性

工业互联网的安全性对制造业、能源等各行业极其重要。工业互联网系统集成了传感器、控制器、数据存储等设备。通过将工业互联网设备连接到网络上实现数据交换和实时监控。然而,连接网络也使工业系统更容易受到恶意网络攻击,从而导致生产中断、设备瘫痪和数据丢失,造成经济损失甚至威胁人身安全。对于工业互联网安全性,了解并应对不同的安全威胁至关重要,安全威胁包括恶意软件、网络入侵、信息窃取以及拒绝服务攻击等。物联网设备的庞大数量和多样性也增加了出现安全漏洞的可能性,因为这些设备可能存在未经修补的弱点。数据的安全性也不可或缺,特别是涉及敏感信息和生产指令的数据^[4]。

随着工业互联网的不断发展,保障其安全性成为各企业和组织关注的焦点。因此,加强安全意识、制定完善的安全政策、实施全面的安全措施、持续监控并应对威胁都是保障工业互联网安全性的关键措施^[5]。工业互联网蜜网因其主动防御和可提前检测未知威胁等特性成为工业互联网安全的一项重要安全机制。

1.1.2 蜜网技术的概念与发展

蜜网技术的概念源于对网络攻击的研究和防御需求,其通过模拟或设置虚假系统资源来吸引潜在的黑客、恶意软件和攻击者,收集关于攻击行为的信息。蜜网最初主要用于识别攻击和保护真实网络设备。随着技术的不断发展,它成为多方面的工具^[6],通过模拟真实网络环境来吸引潜在攻击,攻击者将其注意力从真实目标转移到虚假资源上。同时,蜜网技术在网络安全领域扮演着重要角色,为安全专家提供实验性资源,用以了解和研究不同类型的网络攻击,收集攻击信息和威胁情报,提高网络安全防御能力^[7]。

通过不断地研究和创新,蜜网技术从最初的简单记录攻击行为到如今复杂的交互型蜜网,可更真实地模拟网络环境,对收集数据和了解威胁方式提供了更为详细的信息。蜜网技术的不断发展也满足网络安全战线上持续变化和不断进化的需求。

1.2 蜜网技术原理

1.2.1 蜜网技术的工作原理

工业互联网蜜网通过模拟虚假资源吸引潜在攻击者,记录其攻击行为,并保护真实系统资源的安全^[8],以对后续的网络攻击进行预先的应对。蜜网技术在网络安全领域中是有力的辅助手段,用于识别和应对潜在的网络威胁。工业互联网蜜网工作原理如图1所示。

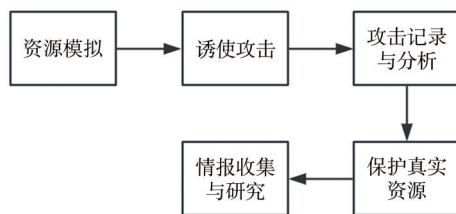


图1 工业互联网蜜网工作原理
Figure 1 Working principle of industrial internet honeynet

1) 资源模拟。蜜网技术首先模拟或设置虚假系统资源,虚假系统资源包括虚拟机、网络端口、文件、数据库等。通过模拟真实资源,可构建逼真的蜜网组成元素^[9]。

2) 诱使攻击。蜜网系统将虚假资源暴露在互联网或内部网络上,以引诱潜在攻击者进入。攻击者通常会扫描网络以寻找易受攻击的目标,

当发现蜜网构建的易受攻击的虚假资源时,会尝试入侵或攻击。

3) 攻击记录与分析。一旦攻击者与虚假资源互动,蜜网系统会记录攻击行为,包括攻击尝试、使用的工具和技术、攻击者的网际互联网协议(internet protocol, IP)地址等。这些信息被用于后续的分析和监测^[10]。

4) 保护真实资源。蜜网技术的关键目标是分散攻击者的注意力和资源,使其专注于虚假资源,从而保护真实系统资源的安全。当攻击者的攻击行为被记录下来时,可及时通知企业管理人员,从而有助于企业采取适当的安全措施来防御潜在的威胁^[11]。

5) 情报收集与研究。收集到的攻击数据可以用于分析攻击趋势、识别新的攻击方法、收集威胁情报等。通过聚合单点蜜网威胁数据,可从单点到多点进行分析,对工业互联网蜜网安全进行研究。

1.2.2 虚拟化与模拟真实系统

蜜网利用虚拟化技术模拟真实的工业设备,包括传感器、控制器、工控设备等。这些虚拟设备在外观和行为上与真实设备相似,可诱使攻击者与其交互。利用设备虚拟化有助于评估攻击者对工业系统特定设备的兴趣和攻击行为。此外,蜜网可创建虚拟网络拓扑,模拟真实工业互联网中的网络结构。通过虚拟化网络组件,蜜网能够观察攻击者在虚拟网络中的行为,深入了解其渗透路径和攻击范围。另外,蜜网使用虚拟化技术模拟整个工业互联网系统,包括操作系统、应用程序和数据库。这使攻击者在虚拟环境中执行的操作与在真实系统中的行为相似,从而有助于收集攻击者对系统漏洞的利用情况以及他们的攻击技术。

尽管蜜网是虚拟环境,但是在模拟中需要实现高真实性。虚拟化组件的行为和特征力求与真实系统相似,使攻击者难以区分虚拟环境和真实环境。这种真实性模拟是为了吸引高级威胁,在虚拟环境中展现其真实的攻击技能。同时,工业互联网蜜网还可通过虚拟化系统组件和模拟各种攻击场景,来还原真实世界中可能发生的攻击情境,以找到潜在威胁和评估防御措施的有效性。

1.3 工业互联网蜜网的优势

工业互联网蜜网技术是用于网络安全的特殊策略，有很多的技术优势，如图2所示。

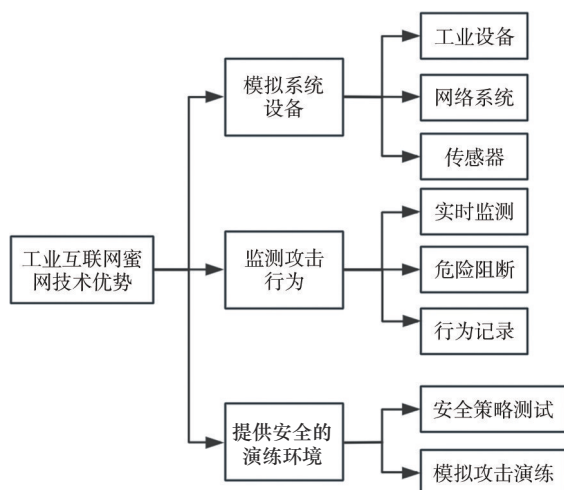


图2 工业互联网蜜网技术优势

Figure 2 Industrial Internet honeynet technology advantages

1) 工业互联网蜜网能够准确地模拟系统设备，包括工业设备、网络系统和传感器，使其看起来像真实设备，增加了攻击者入侵的难度。通过模拟易受攻击的资源，蜜网可以吸引攻击者的关注，使其将精力和资源用于虚假设备，从而减少对真实系统的攻击风险^[12]。

2) 工业互联网蜜网能够实时监测攻击行为，并采取快速响应措施阻止潜在的威胁^[13]。监测攻击可进行危险阻断，有助于最小化真实系统受到的损害，并通过记录攻击行为和攻击者使用的工具，帮助安全团队识别新型攻击方法和潜在威胁^[14]。

3) 工业互联网蜜网提供了安全的演练环境，安全团队可以在其中进行安全策略测试和模拟攻击演练，以增强团队的安全意识和反应能力^[15]。

总体来说，工业互联网蜜网技术能够模拟真实工业互联网设备、吸引攻击者、实时监测并收集数据，为网络安全提供有力的防御手段，降低真实系统受到攻击的风险^[16]。

1.4 工业互联网蜜网技术的应用

1.4.1 工业互联网蜜网技术在实践中的应用案例

工业互联网蜜网在实践中多用于模拟攻击与漏洞挖掘、实时威胁监测与攻击阻断、威胁情报共享与跨组织协同，实践应用关系如图3所示。

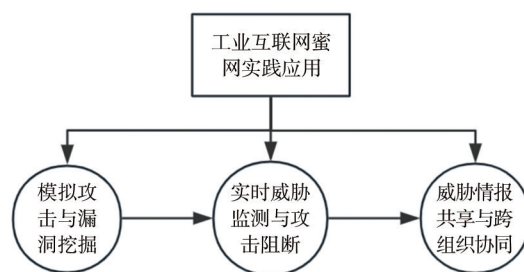


图3 工业互联网蜜网实践应用

Figure 3 Practice and application of industrial internet honeynet

1) 模拟攻击与漏洞挖掘。通过虚拟化供应链中的各个环节，包括制造商、供应商和物流渠道，企业可以评估其供应链的安全性。这种实践有助于发现潜在的供应链漏洞，并采取相应的安全策略，提高整个网络的抗攻击能力。

2) 实时威胁监测与攻击阻断。通过虚拟化工业设备和网络环境，企业能够模拟真实场景中的潜在威胁，并实时监测攻击者与虚拟设备的互动。这种实时监测不仅有助于及早发现异常行为，还能实施及时的阻断措施，有效保障工业系统的稳定运行。

3) 威胁情报共享与跨组织协同。通过模拟虚拟环境中的攻击场景，安全团队能够生成丰富的威胁情报数据。这些数据不仅可以用于本企业的防御，还可与其他组织共享，建立跨组织的威胁情报共享网络，实现更高效、全面的协同防御。

1.4.2 蜜网技术对工业互联网安全的影响

蜜网技术对工业互联网安全的影响体现在多个层面。

1) 蜜网提供了虚假的系统、服务或资源，模拟真实情况^[17]。这样做有助于识别潜在威胁和收集攻击者的情报。通过捕捉攻击者的活动，包括攻击方式、使用的工具、攻击频率等，蜜网可为安全人员提供有价值的情报。通过虚拟化和模拟，蜜网技术减少了真实系统暴露在网络攻击之下的风险^[18]。攻击者更倾向于攻击虚拟环境，使真实生产环境免受直接攻击。蜜网提供了模拟实战的环境，有助于培养和增强员工和安全专家的安全意识。此外，实时的模拟攻击和对攻击者的行为进行分析，可帮助员工深入了解网络威胁。

2) 蜜网技术提供了模拟环境，使安全团队能够进行实时的安全演练和模拟攻击，这有助于

测试安全策略的有效性和系统的防御措施。通过实时记录攻击者的活动，蜜网能够提供安全分析和预警系统^[19]以识别异常活动并向管理员发送警报，使管理员能够及时采取措施应对潜在的威胁。

通过上述功能整合，蜜网成为工业互联网安全的重要工具^[20]，提供了有效的技术手段，有助于发现潜在的威胁、增强安全意识和改进网络防御，并保障工业互联网系统的安全运行^[21]。

2 工业互联网蜜网发展过程

工业互联网蜜网由最初的工控蜜罐逐步发展为工控蜜网，并进行大规模应用，发展为企业级工业互联网及关键基础设施的蜜网。随着技术的进步与发展，蜜罐蜜网的防护能力逐步提升，使整个工业互联网环境更加安全。表1按照时间顺序整理了工业互联网蜜罐蜜网的发展。

2.1 工控蜜罐

工业控制系统是用于监控和控制工业过程的计算机系统，包括用于自动化、监视和控制的设备、传感器、网络和软件。工控蜜罐是特殊设计的安全防护措施，用于保护工业控制系统免受恶意攻击。工控蜜罐的主要目的是吸引攻击者，诱使其攻击蜜罐系统，以便安全团队可以监测和分析攻击行为，从而提高对真实工业控制系统的保护水平。蜜罐通常是模拟真实的工业控制系统，包括虚拟设备、网络和应用程序。它们创建了看似易受攻击的环境，来吸引攻击者尝试入侵和攻击。

工控蜜罐的研究以工控协议为基础，常见的工控协议有S7comm、Modbus、分布式网络协议3（distributed network protocol3，DNP3）、互联网通协议（inter-control center communication protocol，ICCP）、IEC 60870-5-104、对象链接、嵌入过程控制（object linking and embedding for process control，OPC）协议、Ethernet/IP和（factory interface network service）等。随着科技的进步，神经网络技术也正在被应用于蜜罐的使用，下面对常用的OPC和近年来新出现的神经网络蜜罐技术进行详细介绍。

OPC协议是在工业自动化领域中被广泛使用的技术，它允许不同厂商的自动化设备之间进行通信和数据交换。最早是由美国的软件公司OPC Foundation推出的，它通过一系列标准、规范和接口，实现了不同自动化设备之间的数据交换和信息共享。OPC技术已经成为现代工业自动化领域中必不可少的一部分。由于OPC是受业界普遍认可和采纳的通信协议，以OPC协议为主所开发的工控蜜罐成为目前的主流蜜罐类型之一。2019年，Petre等^[22]实现了基于OPC协议的OPC UA的工控蜜罐，并将其应用于水泵站的现实设施，通过对已有的本地自动化部署和SCADA系统进行研究，改善了传统蜜罐对于攻击的检测能力，专注于对蜜罐实现和微机上运行的研究，提出了具有灵活性，能够在本地自动化部署的蜜罐。2023年，Sutton等^[23]实现了基于OPC协议的具有良好性能的蜜罐。蜜罐基于

表1 工业互联网蜜罐蜜网的发展
Table 1 Development of honeypot honeynet of industrial Internet

序号	年份	文献	数据捕获	安全控制	形态	交互程度	资源类型
1	2019	Honeypot inside an OPC UA wrapper for water pumping stations ^[22]	日志	无	蜜罐	高交互	虚拟
2	2020	An IoT honeynet based on multiport for capturing IoT attacks ^[23]	日志流量	沙箱运行与调试	蜜网	高交互 中高交互	虚拟
3	2022	Sensors for detection of cyber threats on industrial environment using a high interaction ICS/SCADA honeynet ^[24]	日志流量	虚拟机隔离与控制	蜜网	高交互 低交互	虚拟 实体
4	2022	Secure and resilient artificial intelligence of things: a honeynet approach for threat detection and situational awareness ^[25]	日志流量	沙箱运行与调试	蜜网	高交互	虚拟
5	2023	NeuPot: a neural network-based honeypot for detecting cyber threats in industrial control systems ^[26]	日志	虚拟机隔离与控制	蜜罐	高交互	虚拟
6	2023	HoneyICS: a high-interaction physics-aware honeynet for industrial control systems ^[27]	日志流量	虚拟机隔离与控制	蜜网	高交互	虚拟

OPC 协议服务器, 可以识别蜜罐作为诱饵过程中输入/输出数据的不一致, 并提出了诱饵过程中可视性的解决方案。

近年来, 神经网络技术逐渐成熟, 也逐渐被应用在工控安全方面。2023 年, Shan 等^[26]基于神经网络技术实现了工控蜜罐。随着攻击者攻击方式的日益复杂, 开发传统的有效识别和响应攻击的工控蜜罐逐渐变得困难, Shan 等^[26]开发了基于神经网络技术的蜜罐 NeuPot, 提高了蜜罐的交互和网络威胁检测能力, 可以根据特定的工业场景响应攻击者的请求, 而无须与 ICS 进行持续通信并检测恶意流量; 并且为了创建这种蜜罐方案, 作者设计了新的 seq2seq 时间序列预测模型, 该模型以 Huber 损失为指导, 以模拟实际 ICS 物理过程的长期变化; 然后, 创建 Modbus 蜜罐框架, 以响应这些 ICS 物理过程与攻击者交互时的变化, 并捕获针对 ICS 的各种网络威胁。此外, 作者还设计了用于工业协议级恶意流量检测的新型丢失函数, 用于识别已知和未知威胁。根据实验对比分析, 所提出的蜜罐方案非常有效, 在交互性和检测网络威胁方面优于较先进的方案。

未来, 蜜罐技术需要成为一个智能代理, 能够反映 ICS 的物理过程的变化, 同时需要限制与 ICS 的信息交换, 以保证 ICS 的完整性和安全性。此外, 大多数现代蜜罐的研究集中在技术方面, 如流量迁移和虚拟化, 而忽略了蜜罐的智能化。因此, 未来蜜罐技术需要更多地关注智能化方面的研究。

2.2 工控蜜网

随着互联网技术的快速发展, 越来越多的工业设备接入互联网中, 使工业能力相较过去有了显著提升, 但是由于缺乏有效的防护机制, 工控系统受到攻击的报告日益增加, 作为一种以低错误检测率获取有关攻击者行为的有用信息的方式, 蜜罐在网络安全领域取得了重大进展。但仅依靠现有的蜜罐技术对工控系统进行保护, 并不能取得较为理想的效果, 鉴于此, 蜜网技术应运而生。

蜜罐在浪费攻击者资源和吸引其在网络中其他关键资产的注意力方面很强大。具有多个蜜罐的欺骗性网络称为蜜网。蜜网中的蜜罐旨在相互

合作以增加它们的欺骗能力。专业攻击者利用强大的检测机制来检测网络中蜜罐的存在。当攻击者发现部署了欺骗机制时, 它可能会改变其行为并对网络造成恶意影响。因此, 蜜网必须具有足够的欺骗性才能不被识别^[28]。

而工控蜜网通过模拟仿真、诱捕技术, 能够对国内工业资产进行探测, 并对情报收集行为以及各类攻击行为进行有效监测。针对当前工业蜜罐交互能力差、伪装度低的弱点, 蜜网的仿真环境能够对蜜罐工业系统伪装能力进行有效的技术补充。

通过模拟工业企业边界系统及相关资产, 引导攻击流量进入蜜网, 诱使攻击者对蜜网系统及相关资产进行扫描探测与攻击尝试, 能够有效地保护工业企业真实系统及相关资产, 在降低企业遭受攻击风险的同时, 对攻击者的攻击手段及意图进行深度分析, 从而提升工业企业系统的安全防护能力和技术水平。通过持续的蜜网数据分析和攻击行为监测, 制定针对性防护策略, 实现完善工业控制系统缺陷, 提高区域工业控制系统安全防护水平, 帮助企业完善自身防护能力建设和提高企业安全防护技术能力建设^[29]。目前主流的企业级工控蜜网, 通过模拟企业生产系统中的 Web 系统, 实现多方威胁诱捕^[30]。

为了应对更加复杂的端口攻击, 2019 年, Zhang 等^[31]设计并实现了基于多端口蜜罐的蜜网来抓取物联网中的攻击。由于物联网的网络资源有限且操作系统复杂, 容易受到攻击。Zhang 等^[31]首先在 CVE-2017-17215 漏洞的基础上, 实现了中高交互蜜罐, 可以模拟特定系列的路由器通用即插即用 (universal plug and play, UPnP) 服务, 具有业务模拟、日志记录、恶意样本下载和业务自检等功能。并且鉴于模拟 UPnP 服务可用的细节有限, 为了帮助蜜罐响应无法识别的恶意请求, 使用与漏洞匹配的实际物联网设备固件来构建高交互蜜罐。Zhang 等^[31]还研究了简单对象访问协议 (simple object access protocol, SOAP) 服务端口, 设计了相应的多端口蜜罐, 以增大蜜网的容量, 从真实设备提供混合服务并模拟蜜罐, 最后制作了蜜网中的 Docker 镜像, 减小了蜜罐的体积, 实现了蜜网的快速部署, 封

装了所有这些蜜罐,使蜜网控制中心可以将命令和文件同时传输到蜜网中的每个物理节点。此外,2022年,Campos等^[24]研究实现了专为实时控制环境设计的蜜罐和蜜网作为防止网络攻击的工具,并生成有助于改进ICS/SCADA环境中网络安全和异常检测技术的统计数据。高交互性ICS/SCADA蜜网可以被视为传感器,用于维护最新的攻击签名技术基础,帮助识别信息和工业自动化系统中的漏洞,并促进攻击证据的保存,以供将来进行取证分析。

然而,由于工控蜜网其独有的特性,不同厂商之间的设备在网络协议、文件系统、服务端口等多个方面有较大的差异,为了实现不同设备之间的兼容,现有研究对于工控蜜网做了很多有成效的工作。但是随着技术发展,出现了越来越多的攻击方式,设计传统的能提供有效安全防护的蜜网逐渐变得困难,现有的工控蜜网工作在这方面也并未达到理想状态。

2.3 企业级工业互联网及关键基础设施的蜜网

工业互联网系统作为国家关键基础设施的重要组成部分,很容易成为国家间网络对抗和有组织黑客攻击的目标。根据Franco等^[32]的研究,蜜罐蜜网在基础设施上的应用类型大致分为智能电网、供水系统和燃气管道等方面。随着在这些应用领域中使用蜜网技术并不断深入研究,对工业互联网攻击的理解不断提高,蜜网逐渐被应用于工业互联网的防护,成为工业互联网安全领域重要的工具。

相较普通的蜜网,企业级工业互联网蜜网更侧重在真实环境的可扩展特性和满足在虚拟环境的低侵入的要求。在普通蜜网的基础上,企业级工业互联网蜜网更侧重于使用工业互联网仿真环境和生产环境建模、攻击诱捕导流、攻击行为判定等核心技术,进行威胁数据采集、攻击行为诱捕及溯源分析^[33]。目前主流的企业级工业互联网蜜网应用较多的是通过模拟企业生产系统中的Web系统^[33],引诱攻击者进入蜜网模拟的隔离区,横向移动进入模拟的企业办公网络进行攻击,以此收集和分析攻击行为。

然而,工控领域的特殊性,工控系统的网络结构、通信协议、设备等多方面的独特性,导致

现有检测方法出现漏报率、误报率较高等问题,较难检测真实发生的攻击行为^[34]。面对这些威胁时,蜜罐和蜜网对于了解和抵御工业互联网攻击至关重要,它们可以吸引并欺骗攻击者,使其误以为已经成功侵入真实系统。通过识别、分析以及收集攻击者的行为和信息,可以改进和提高系统的安全性。蜜罐与其他安全措施相结合,形成蜜网这样的综合安全体系,才能更好地应对威胁。

Lucchese等^[27]提出了名为HoneyICS的ICS蜜网,可在很大程度上模拟真实工业网络中的细节。HoneyICS支持可编程逻辑控制器(programmable logic controller, PLC)和人机界面(human machine interface, HMI)种类的蜜罐,相比大多数现有框架更加强大。HoneyICS支持高扩展性,因为它能够模拟不同品牌的PLC和ICS协议,所以PLC仿真包括对常见工业网络协议的精确仿真;HoneyICS允许攻击者修改PLC寄存器的值,并支持模拟连接到PLC的物理工厂,因此可以为攻击者的命令提供真实的反馈;HoneyICS可进行由蜜罐管理员精确监控的重要中间人攻击。另外,Tan等^[25]在2022年提出了使用人工智能构建的蜜网,该蜜网为了应对工业4.0时代日益复杂的攻击方式,摆脱传统蜜网的局限,使用以人工智能为基础的蜜网系统,提高了蜜网的安全性,使蜜网拥有了威胁检测和态势感知功能,增强了人工智能物联网的安全性和弹性。Tan等^[25]设计的蜜网可以将收集到的攻击数据转换为图像,并用作训练深度学习模型的样本。

综上所述,蜜罐是重要的安全防护工具。随着工业设备接入互联网数量的增加,工业互联网面临着越来越多的攻击。为了应对这一问题,企业级工业互联网蜜罐提供了核心技术,如工业互联网仿真环境、攻击诱捕导流和攻击行为判定,用于威胁数据采集、攻击行为诱捕和溯源分析。在实施企业级工业互联网蜜罐时,可以选择蜜网类蜜罐,蜜网类蜜罐模拟了企业生产系统中的Web系统,可以诱使攻击者进入模拟的系统,并进行横向移动。对于关键基础设施的安全,蜜网也可以提供态势感知和威胁检测的功能。鉴于当前神经网络、人工智能等技术的成熟和普及,蜜网与这些技术相结合成为研究热点,未来这种研

究会越来越多,蜜网会逐渐向着更加智能化、更加安全的方向发展。

3 工业互联网蜜网平台

随着虚拟化技术的发展,工业互联网蜜网系统从传统的硬件蜜网发展成动态灵活的虚拟化蜜网。本节详细介绍设备仿真、协议模拟仿真和部署分析的仿真方法。

3.1 设备仿真

设备仿真是指通过计算机模拟和仿真技术创建虚拟设备,可以对工业互联网蜜网系统中设备的运行状态、通信行为和故障状态等进行虚拟建模和评估。相比真实设备,构建设备仿真具有以下两个优势:一是设备仿真不需要实际的硬件或组件,成本较低;二是设备仿真可以轻松修改和重新配置,允许用户测试不同的场景和配置,无须进行物理重连。因此,通过构建设备仿真,可以有效部署蜜网并提升工业互联网的安全性。其中,设备仿真主要分为虚拟化和软硬件模拟两类。

1) 虚拟化。比较成熟的技术包括 x86 架构的虚拟化、Docker 容器化技术、Mininet 仿真器等。其中, x86 架构的虚拟化技术是指将一台物理机器分割成多个虚拟机,在每个虚拟机上运行不同的操作系统和应用程序。这种虚拟化技术可以提高硬件资源利用率,简化系统管理,实现应用程序的快速部署。常见的 x86 虚拟化技术包括 VMware、VirtualBox、基于内核的虚拟机(kernel-based virtual machine, KVM)等。Docker 容器化技术是轻量级的容器化技术,它是基于 Linux 内核的 cgroups 和 namespace 机制实现的。Docker 可以将应用程序及其依赖项打包成一个独立的容器,使应用程序在任何环境中运行,提高了应用程序的可移植性、可伸缩性和安全性。常见的 Docker 容器化技术包括 Docker Engine、Kubernetes、OpenShift 等。Mininet 仿真器可以在单个计算机上模拟出网络环境,包括多个主机、交换机和路由器。Mininet 可以用于网络协议的研究和测试,以及网络应用程序的开发和测试。Mininet 仿真器的优点是可以在相对较小的环境中进行大规模网络的测试和调试,而不需

要大量的硬件设备。通过虚拟化技术,蜜网可以实现虚拟化运行。

2) 软硬件模拟。比较成熟的技术有 PLC、SCADA、HMI 等虚实互联技术。其中, PLC 是可编程逻辑控制器,通过软件仿真来进行逻辑程序的开发和测试,以验证逻辑控制的正确性。SCADA 用于监视、控制和采集工业生产过程中的数据。它通常由远程终端单元、传感器、控制器和人机界面组成,可以使用软件仿真来模拟实际工业过程验证监视和控制功能的正确性。HMI 是用户与机器或系统进行交互的界面。它可以通过软件仿真来模拟用户与系统的交互过程验证界面设计和功能。利用软硬件模拟,可构建高逼真的蜜网设备虚实互联,实现一致性反馈蜜罐。

2013 年, Beham 等^[35]比较了现有的嵌套虚拟化解决方案的性能,并分析了性能开销对基于虚拟机监控技术的入侵检测和蜜罐系统的影响;通过评估性能开销得出结论,提供了在嵌套虚拟化环境中进行有效入侵检测和蜜罐的方法。但当时该虚拟化仍处在起步阶段。2018 年, Kyriakou 等^[36]在容器化平台 Docker 上运行蜜网,构建了快速的多组件系统,使其具有轻量级、弹性、易于部署和管理方便等特点,为研究人员提供了丰富的数据。未来将会在更多地方部署蜜罐,并用其支持更多协议,找到更好更合适的虚拟化设备。2020 年, Mashima 等^[37]将 Mininet 作为其中一个虚拟网络环境,模拟智能电网系统的通信基础设施,帮助作者评估蜜罐系统的真实性和功能,并计划将该系统下得到的数据应用到入侵检测等方面。

此外, 2018 年, Conpot 蜜罐基于收集到的攻击者的动机和攻击方法的数据,实现针对 ICS 和 SCADA 系统的仿真^[38]。2023 年, Chowdhury 等^[39]设计并实现了名为 PLCHoney 的虚拟 PLC 蜜罐, PLCHoney 采用 Docker 虚拟 PLC,模拟真实 PLC 的所有任务,包括在扫描周期中运行应用程序、从传感器获取输入数据,以及更新输出数据来控制物理过程等。未来会对该模型的真实性和准确性进行进一步研究。2023 年, Yang 等^[40]提出了高交互蜜罐,采用高交互的蜜罐和模块化的设计思路,将蜜罐环境与数据处理的中心节点区分开来,可用于模拟和监测攻击者对工业控制系

统的攻击行为。未来还会支持更多工业网络协议, 并对物理过程采用轻量级仿真。

综上所述, 工业互联网蜜罐设备仿真是有效的安全工具, 可以模拟和模仿真实的工业控制系统环境, 主要用于引诱攻击者、收集攻击数据和情报、提供早期攻击检测以及增强安全意识和培训。它对于保护工业互联网系统的安全性和稳定性具有重要作用。未来学者对协议支持和仿真轻量化等方面进行改进, 这将有助于提高工业互联网蜜罐设备仿真的效率和可操作性, 从而更好地保障工业互联网系统的安全性和稳定性。

3.2 协议模拟仿真

工业控制协议是用于工业自动化领域的通信协议, 是工业控制系统中不同设备之间进行信息交换和数据通信的基础。可靠的工业控制协议能够为工业生产提供高效、稳定、可靠的数据通信方式, 对提高工业生产的自动化水平具有重要意义。在蜜网系统中, 为有效抵御对蜜网的识别, 通常需要对工业控制协议实施模拟仿真。以 Modbus、S7Comm (S7) 和 IEC104 协议为例, 对协议模拟仿真相关技术进行如下分析。

1) Modbus 是广泛用于各种工业控制系统的通信协议, 最初由 Modicon 公司 (Schneider Electric) 发布, 用于 PLC。它现在已经成为工控领域通信协议的业界标准, 因此对实现 Modbus 工控协议仿真的蜜罐系统研究具有重要意义。Pothamsetty 等^[41]发布了第一款 PLC 蜜罐, 通过使用传统蜜罐系统的 Honeyd 架构工具配置获取 Nmap 和 Xprobe 签名文件, 并将数据包响应发送到与这些签名匹配的扫描中, 以此来模拟仿真 Modbus 工业控制协议, 第一次实现了在端口 502 上模拟 Modbus/TCP 服务器, 能够响应 Modbus 多种基础功能码。Haney 等^[42]设计了轻量级的 SCADA 蜜罐框架, 基于 JAMOD 开发组件部署网络节点, 以此实现 Modbus 通信协议的简单逻辑和变量控制, 来模拟使用 Modbus 协议的 PLC, 以及可能在现代 PLC 上找到的各种管理界面和组件。不足的是, 这个蜜罐框架是中低交互的。Vasilomanolakis 等^[43]认为对 Modbus 的正确行为进行建模, 需要模拟 Modbus 系统对 Modbus 主设备发出命令的响应。此方法采用预设指令集和存

储块值来模拟 Modbus 协议的通信过程, 其能够响应大部分 Modbus 请求报文, 并逃避侦察工具的检测, 但是基于模板的交互机制很容易被攻击者识别。Siniosoglou 等^[44]提出了深度学习 Modbus 蜜罐框架, 该框架通过建立实现 Modbus 协议服务的蜜罐增加物理过程交互仿真, 模拟具有时间属性的细粒度物理过程参数, 增强蜜罐的欺骗能力。

2) S7Comm 是西门子 S7 系列 PLC 内部集成的通信协议, 也是 S7 系列 PLC 的精髓所在。S7 协议的 TCP/IP 实现依赖于面向块的 ISO 传输服务。S7 协议被封装在 TPKT 和 ISO-COTP (connection-oriented transport protocol) 中, 这使协议数据单元 (protocol data unit, PDU) 能够通过 TCP 传送。Lau 等^[45]提出了全新的 S7 协议蜜罐交互标准, 并基于该标准设计出了 XPOT 蜜罐系统。该系统依照西门子 S7-314C-2 PN/DP 型号 PLC, 通过 MC7 字节码编程实现 PLC 程序执行及调试功能, 并使用底层虚拟机优化技术逼近真实 PLC 程序编译用时。Xiao 等^[46]开发了高交互的工业控制系统蜜罐——S7commTrace。在 S7 通信协议仿真模块中, 根据协议格式对接收到的数据进行解析得到有效内容, 然后参照用户模板生成回复数据, 再传回 TCP 通信模块进行打包。实验结果表明, S7commTrace 在协议仿真中支持更多的函数, 提高与攻击者的交互深度, 可以有效诱发更多高层攻击。Ding 等^[47]提出了高交互作用的 S7 蜜罐。基于 IMUNES 来模拟网络, 但不在网络节点上安装 Conpot, 而是使用 SNAP7 库获得具有模拟 S7 通信和简单网络管理协议 (simple network management protocol, SNMP) 的网络节点的高交互 ICS 蜜网。

3) IEC104 全称为 IEC 60870-5-104 协议, 它是基于 TCP/IP 传输的网络协议, 是专为电力装置和电网设计的远程控制和通信标准。Redwood 等^[48]通过扩展 Conpot 来模拟 IEC 61850 数字通信协议, 并将 IEC 61850 中的 MMS (manufacturing message specification)、GOOSE (generic object oriented substation event) 和 Modbus 协议实现为抽样服务以支持基础设施建模层参与者和人机界面之间的交互; 然后通过对智能电子设备二进制

文件进行工程和逆向工程, 保证 ICE 61850 协议仿真模块的高度交互。Grammatikis 等^[49]提出的 SDN-microSENSE 提供多种 EPES/SG 蜜罐系统, 可实现对 IEC 61850、IEC 60870-5-104 和 Modbus/TCP 这 3 种 EPES/SG 通信协议的仿真。其中, IEC 61850 蜜罐通过解析智能功能描述文件来模拟变电站断路器中的真实智能电子设备。IEC 60870-5-104 和 Modbus/TCP 蜜罐则是基于 Conpot 技术来实现的。Ferretti 等^[50]部署了一组基于 Conpot2 的低交互蜜罐, 并公开了一组有代表性的 ICS 协议; 通过对 Conpot 进行扩展, 重新实现了 BACnet 协议, 改进了 EtherNet/IP、IEC104 和 Siemens S7 的实现; 同时去除可用于对蜜罐进行指纹识别的 Conpot 特征, 使之更真实地模拟真实设备, 提高 ICS 协议实现的准确性。

在蜜网系统中, 协议仿真的精确性尤其重要, 工控协议的仿真需要准确地模拟协议的行为和通信过程, 以至于攻击者错误地认为自己找到的蜜网是可以被攻击的真实系统, 但现有工控蜜罐普遍存在工控协议扩展困难和工控业务仿真复杂的问题, 仿真结果可能存在一定的误差。

3.3 部署分析

工业互联网蜜网是发现工业互联网攻击和潜在威胁的重要手段, 在实际使用过程中需要对仿真的设备和协议进行部署后, 对产生的数据进行分析, 但是, 面临着工业互联网系统复杂难以部署和数据量大且特征不明的问题。在工业互联网蜜网部署中, 要对真实的业务流程进行模拟, 来诱导攻击者进行攻击。其流程中不仅包括设备模拟和协议模拟, 还包括网络传输和物理操作过程。数据分析是对工业互联网蜜网诱捕产生的日志等数据进行处理, 来挖掘其中的攻击信息。

工业互联网蜜网部署通过集中管理、重定向和虚实蜜罐相结合等技术对蜜网结构进行部署。2019 年, Bernieri 等^[51]提出了名为 MimePot 信息物理蜜网。它可以直接连接到工厂网络, 具有模拟物理过程操作的能力, 并且基于线性时不变模型对 ICS 组件和控制程序进行仿真。该方法的目标是引诱具有控制理论知识的熟练攻击者, 并且使用配水系统仿真展示了初步结果。蜜网出现之后, 也出现了针对蜜网的攻击手段, 如反蜜罐攻

击。反蜜罐攻击是指攻击者采取各种手段来检测、规避或干扰蜜罐和蜜网的部署, 在反蜜罐攻击中, 攻击者首先判断防御系统中蜜罐是否存在, 然后攻击者再识别防御系统中部署的蜜罐类型, 通过蜜罐类型来破坏蜜网诱捕和防御。2019 年, Du 等^[52]提出了伪蜜罐博弈策略来保护 SDN 免受基于反蜜罐的攻击。通过多阶段模型的博弈, 使用伪蜜罐来应对反蜜罐攻击, 更好地伪装了真实蜜罐。他们还证明了该策略可以在合法用户和攻击者之间实现最佳平衡从而提高防御效率。主动部署是为了应对攻击者变化的攻击策略而提出的, 2020 年, Zarca 等^[53]提出了基于 SDN 和网络功能虚拟化 (network function virtualization, NFV) 的工业互联网蜜网策略部署, 他们模拟了真实的物联网传感器的网络, 攻击者被重新定向到该网络以分散注意力和进行调查, 从而抵消其攻击的损害。与传统解决方案不同, 该方法中蜜网不仅可以主动部署, 还可以根据反应模块提供的反应, 被动地作为缓解网络攻击的对策。此外, 蜜网中的连接和数据控制通过 SDN 集中管理。SDN 控制器负责提供流量过滤和转发, 以及重定向机制, 根据入侵调查的需要, 将流量连接从真实物联网网络转移到虚拟物联网蜜网。在动态部署的基础上进行虚实蜜罐结合的工业互联网蜜网具有综合的应对能力, 2022 年, Zheng 等^[54]提出了虚拟与现实相结合的新型蜜罐系统架构。系统可根据受保护网络状况, 动态地生成大而高的仿真陷阱。蜜网可以欺骗攻击者, 并在整个攻击过程中根据攻击者的行为动态调整网络拓扑以及节点的组成和类型。

工业互联网蜜网数据分析是通过综合运用大数据技术、异常检测和物联网设备, 对工业互联网蜜网中的数据进行系统性分析的过程。2019 年, Triantopoulou 等^[55]设计网络协议嗅探器和基于签名的攻击分析工具, 以捕获数据包, 并识别分析恶意活动。针对 DDoS 攻击来分析安装在互联网服务提供商 (Internet service provider, ISP) 边缘路由器上的蜜网系统的数据, 并针对分析提出缓解趋势攻击媒介的策略。2020 年, Boukela 等^[56]提出以局部异常因子为基本算法的异常值集成, 通过改变数据特征子集和异常检测算法的参

数化来改进蜜网数据中的无监督异常检测,实现对异常数据的高效检测。2022年,Tok等^[57]使用辅助工具对包括蜜罐日志在内的原始数据进行处理来减少数据量,并将原始数据转换为结构化数据集,然后将数据集导入Hadoop环境中进行分析,通过比较分析来确定可能的僵尸网络活动,并通过Hadoop-Power BI集成将结果可视化为图表和热图。2023年,Mudgal等^[58]提出了名为大数据入侵检测与蜜罐智能系统(big data intrusion detection and honeypot intelligent system, BDE-IDHIS)的入侵检测方法。BDE-IDHIS方法首先检测蜜罐数据中的异常,然后将流量转移到系统,以确保实际系统的有效安全;并且,使用了带有决策引擎和重定向引擎的消息队列遥测传输蜜罐,检测了蜜罐的异常数据,对数据进行了安全处理。

4 工业互联网蜜网评估体系

工业互联网蜜网是专门用于工业互联网环境的安全措施,它通过模拟真实工业互联网环境来吸引潜在攻击者,收集关于工业系统中可能的威胁和攻击方法的信息。为了分析不同蜜网的能力,本文提出了基于Adversarial Tactics, Techniques & Common Knowledge (ATT&CK)的企业矩阵模型的蜜网评估体系,ATT&CK的企业矩阵模型如图4所示。

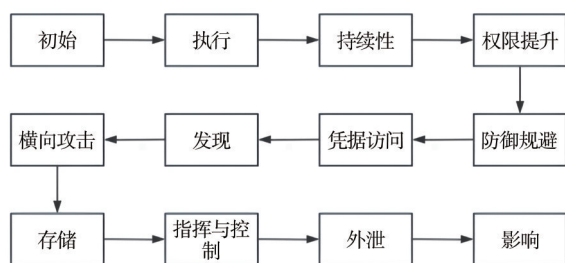


图4 ATT&CK的企业矩阵模型
Figure 4 ATT&CK's enterprise matrix model

4.1 ATT&CK的企业矩阵模型

MITRE ATT&CK是用于描述和组织攻击行为的框架。ATT&CK的企业矩阵是该框架中的一部分,专注于企业网络中的威胁行为。如图4所示,ATT&CK的企业矩阵由“初始—执行—持续性—权限提升—防御规避—凭据访问—发现—横向攻击—存

储—指挥与控制—外泄—影响”12个过程组成。MITRE ATT&CK框架的企业矩阵于2015年首次被提出。ATT&CK最初是用于描述持续性威胁(advanced persistent threat, APT)行为的框架。2020年,Qi等^[59]使用ATT&CK框架设计网络攻防测试平台攻击分析框架。2023年,Hobert等^[60]使用ATT&CK框架对Linux Shell蜜罐上的行为相似性进行检测来增强网络归因。通过MITRE ATT&CK框架研究攻击者行为并确定其战术、技术和程序之间的相关性,可以在不同攻击事件之间建立联系来获得有价值的见解,以补充网络归因。

4.2 基于ATT&CK的企业矩阵模型的蜜网评估体系

工业互联网的复杂特性导致工业互联网蜜网评估困难。现有评估体系多从实现原理和部署难易方面评价,存在评估范围小和评估不完全的问题。本文通过ATT&CK的企业矩阵把工业互联网蜜网的组成进行拆分。基于ATT&CK的企业矩阵模型的蜜网评估体系如图5所示,拆分成环境部署、信息整合、感知分析和智能辅助4个部分,并对这4个部分进行了评估要素细化。

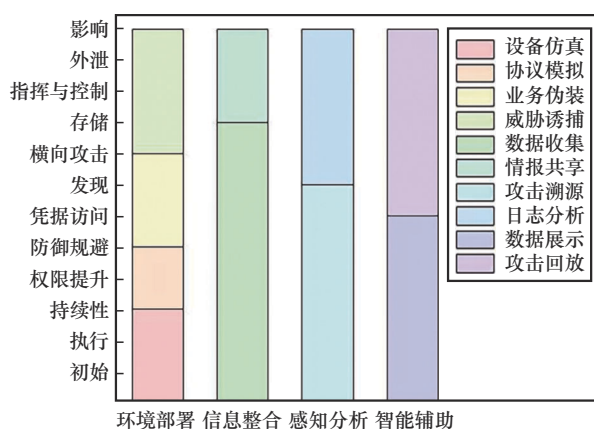


图5 基于ATT&CK的企业矩阵模型的蜜网评估体系
Figure 5 Honeynet evaluation system based on ATT&CK enterprise matrix model

在环境部署方面,评估分为设备仿真、协议模拟、业务伪装和威胁诱捕4个要素。在工业互联网蜜网系统中,设备仿真是一项重要的技术,用于模拟和模仿真实工业环境中各种设备的行为和互动。设备仿真指标是对蜜网中的工控主机、边缘设备和控制器等设备仿真的完整性和可用性进行评估。协议模拟仿真是对工业互联网复杂设

备之间的不同通信协议进行模拟仿真。协议模拟仿真指标是对工业互联网协议的模拟和主机之间的通信进行评估。业务伪装目的是把蜜网伪装成正常运行的业务系统,来吸引攻击者。业务伪装指标是从真实的业务功能和流量方面进行评估。威胁诱捕通过故意暴露虚假的系统或服务,以吸引和识别潜在的攻击者。威胁诱捕指标是通过分析诱导攻击者与其互动,从而获取攻击手法、恶意代码和攻击者身份等信息进行评估。

在信息整合方面,评估分为数据收集和情报共享两个要素。在工业互联网蜜网系统中,数据收集是通过监控、记录和分析攻击者与蜜罐互动的过程,以获取有关攻击手法、恶意代码、攻击者身份等方面的信息。数据收集指标是对蜜网收集信息的完整度和日志记录的准确度进行评估。蜜网系统中的情报共享是指将在蜜网环境中收集到的关于攻击者、攻击手法、漏洞利用等信息的共享。情报共享指标是对蜜网情报共享的延迟度和分配准确度进行评估。

在感知分析方面,评估分为攻击溯源和日志分析两个要素。蜜网的攻击溯源是指追踪和记录在蜜网环境中攻击者的行为,以了解攻击者的策略、目标和技术手法。它关注于分析攻击者在虚拟或模拟环境中的活动。攻击溯源指标是对蜜网

追踪攻击效果进行评估。蜜网的日志分析是指审查和分析蜜网系统产生的各种日志,以获取关于攻击者行为和系统响应的信息。它涵盖了更广泛的数据源和分析维度。日志分析指标是对蜜网系统日志分析范围和日志分析结果进行评估。

在智能辅助方面,评估分为数据展示和攻击回放。蜜网的数据展示是指通过可视化等手段,将蜜网系统中的各种信息以直观的方式呈现给安全团队,辅助安全团队进行维护。数据展示指标是对数据展示直观程度和攻击者画像构建等方面进行评估。蜜网的攻击回放是指通过重新模拟或回放蜜网环境中的模拟攻击过程,以便深入分析攻击者的行为、攻击路径和使用的工具。攻击回放指标是蜜网对攻击路径、命令和时间轴等要素的回放进行评估。

工业互联网蜜网能力评估如图6所示。在环境部署方面,大部分工业互联网蜜网能对环境进行有效部署,并设置相应的业务流程。在信息整合方面,大部分蜜网可以做到信息收集,但是基本达不到信息共享,使蜜网信息不公开,导致攻击者的重复攻击。在感知分析方面,所统计的蜜网大多可以对日志进行分析,但是攻击溯源工作部分缺失。在智能辅助方面,大部分蜜网无法做到数据展示和攻击回放,这方面需要后续完善蜜网的完整性。

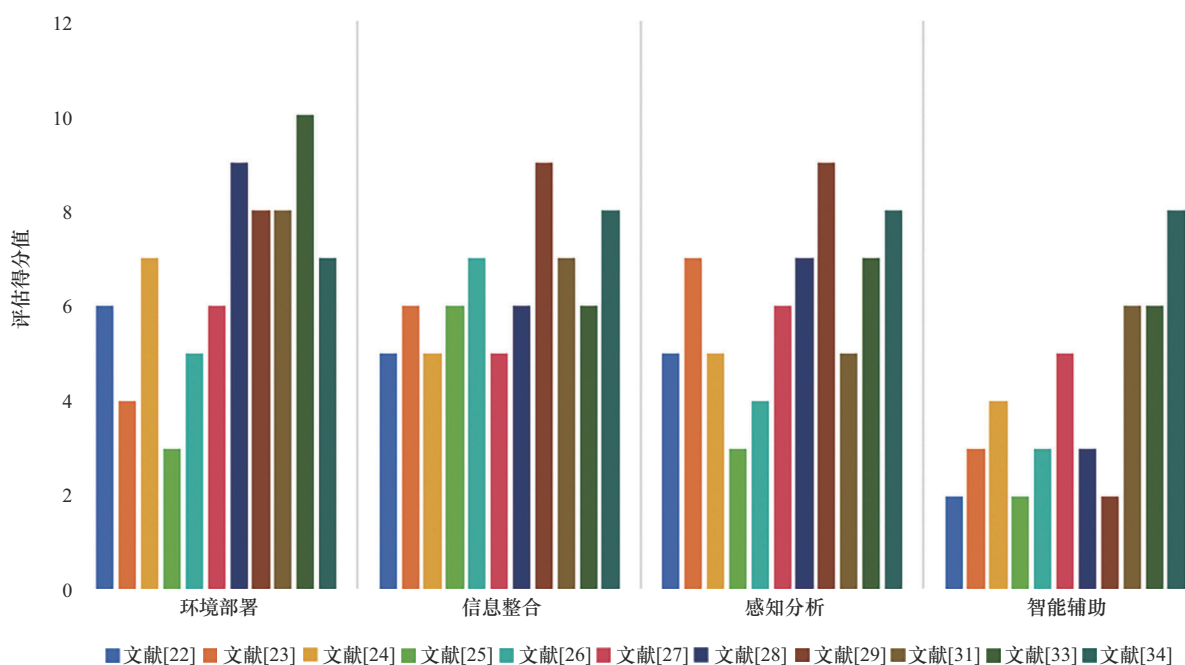


图6 工业互联网蜜网能力评估
Figure 6 Industrial Internet honeynet capability assessment

5 结束语

本文深入阐述了工业互联网蜜网的原理、安全性、优势和评估体系。以PLC、SCADA和HMI等关键工控组件仿真技术为基础,介绍了企业级工业互联网和关键基础设施的蜜网的保护方法。蜜网仿真资源可通过模拟工业互联网中的软硬件,诱导攻击者攻击流量进入蜜网的模拟环境,从而使蜜网有助于分析攻击者流量,并了解攻击者的动向。此外,本文介绍了神经网络技术在蜜罐和蜜网中的应用,神经网络技术扩展了传统蜜罐和蜜网的能力,实现了态势感知和威胁检测功能;介绍了工业互联网中蜜网的部署策略。考虑到实际工业环境的复杂性与独特性,为了实现工业互联网中存在的攻击和威胁的检测,蜜网的部署策略也因地制宜,以期能够发挥蜜网最大的能力。同时,本文还提出了工业互联网蜜网评估体系,从4个部分对工业互联网蜜网的能力进行评估,为用户快速且全面地了解工业互联网蜜网提供了有力帮助。

随着工业互联网的迅速发展,网络威胁不断升级,攻击手法日益复杂。未来的研究方向既充满挑战又蕴藏机遇,应该着重于多个方面。

1) 新兴协议的安全性研究。随着物联网和工业互联网的融合,新兴协议的安全性将成为研究的热点,特别是对象链接和嵌入过程控制协议等在物联网设备中的广泛应用,对其安全性的深入研究将有助于提出相应的防御措施。

2) 重点行业工控安全。重点行业设备的关键性使其成为攻击目标。未来的研究应该集中在重点行业所采用的工控协议的安全性上,以确保重点行业设施的可靠性和安全性。

3) 工控设备漏洞研究。针对工控设备的漏洞研究将更为深入,特别是重点行业设备中较为常见的协议。研究人员应提出修复和防御这些漏洞的解决方案,以确保工控设备的安全性。

4) 网络视频监控设备安全性。鉴于网络摄像头漏洞频发,未来的研究可以更深入地研究与工业互联网相关的协议和设备的安全性,提出有效的防御措施,保障网络视频监控设备的安全性。

5) 区域和组织攻击行为研究。对不同区域

和组织的攻击行为进行更深入的研究,了解其攻击动机和目标。这将有助于建立更为全面的国际合作机制,应对跨国网络威胁。

6) 威胁趋势异常分析。深入研究威胁趋势异常,尤其是针对新兴协议的监测扫描行为。及早发现并理解这些异常趋势,有助于制定更为灵活和有效的网络安全策略。

7) 未来研究还可以关注对蜜网系统的持续优化和改进。包括但不限于提升蜜网节点的真实性,加强蜜网系统的欺骗性能,以更好地吸引攻击者,减少误报的可能性。同时,加强蜜网系统的安全性,防范攻击者对蜜网系统本身的攻击。

综合而言,未来针对工业互联网蜜网技术的研究将在多个方向展开。这需要全球范围内的协作,才能更好地理解和应对不断演变的工业互联网威胁。

参考文献:

- [1] MASOOD R, UM-E-GHAZIA, ANWAR Z. SWAM: stuxnet worm analysis in metasploit[C]//Proceedings of the 2011 Frontiers of Information Technology. Piscataway: IEEE Press, 2011: 142-147.
- [2] TAKAGI H, MORITA T, MATTA M, et al. Strategic security protection for industrial control systems[C]//Proceedings of the 2015 54th Annual Conference of the Society of Instrument and Control Engineers of Japan (SICE). Piscataway: IEEE Press, 2015: 986-992.
- [3] BINNAR P, DALVI A, BHIRUD S, et al. Cyber forensic case study of waste water treatment plant[C]//Proceedings of the 2021 IEEE Bombay Section Signature Conference (IBSSC). Piscataway: IEEE Press, 2021: 1-5.
- [4] SHENG C, YAO Y, FU Q, et al. Study on the intelligent honeynet model for containing the spread of industrial viruses[J]. Computers & Security, 2021, 111: 102460.
- [5] LÓPEZ-MORALES E, RUBIO-MEDRANO C, DOUPÉ A, et al. HoneyPLC: a next-generation honeypot for industrial control systems[C]// Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security. New York: ACM, 2020: 279-291.
- [6] ILG N, DUPLY S, SISEJKOVIC D, et al. A survey of contemporary open-source honeypots, frameworks, and tools[J]. Journal of Network and Computer Applications, 2023, 220: 103737.
- [7] 游建舟, 吕世超, 孙玉砚, 等. 物联网蜜罐综述[J]. 信息安全学报, 2020, 5(4): 138-156.
- [8] YOU J Z, LYU S C, SUN Y Y, et al. A survey on honeypots of Internet of things[J]. Journal of Cyber Security, 2020, 5(4): 138-156.
- [9] KONG T, WANG L M, MA D H, et al. Automated honeynet deployment strategy for active defense in container-based cloud[C]// Proceedings of the 2020 IEEE 22nd International Conference

- on High Performance Computing and Communications, IEEE 18th International Conference on Smart City, IEEE 6th International Conference on Data Science and Systems (HPCC/SmartCity/DSS). Piscataway: IEEE Press, 2020: 483-490.
- [9] WANG Z Q, LI G F, CHI Y P, et al. HoneyNet construction based on intrusion detection[C]//Proceedings of the 3rd International Conference on Computer Science and Application Engineering. New York: ACM, 2019: 1-5.
 - [10] ZUZČÁK M, BUJOK P. Using honeynet data and a time series to predict the number of cyber attacks[J]. Computer Science and Information Systems, 2021, 18(4): 1197-1217.
 - [11] KALININ M, ZEGZHDA D, ZAVADSKII E. Protection of energy network infrastructures applying a dynamic topology virtualization[J]. Energies, 2022, 15(11): 4123.
 - [12] BAKER B, KELSEY Q, JASON P. Machine learning classifiers in honeynets: a critical review[J]. International Research Journal of Engineering and Technology, 2020(7): 6850-6853.
 - [13] LUCCHESI M, MERRO M, PACI F, et al. Towards a high-interaction physics-aware honeynet for industrial control systems[C]//Proceedings of the 38th ACM/SIGAPP Symposium on Applied Computing. New York: ACM, 2023: 76-79.
 - [14] MARYDAS M, PRIYAH J N V. A cloud based honeynet system for attack detection using machine learning techniques[J]. International Research Journal of Engineering and Technology (IRJET), 2019, 6(7): 330-335.
 - [15] DU X Y, ZHOU G Y, WANG Y J, et al. A lightweight honeynet design in the Internet of things[C]//Proceedings of the 2022 IEEE International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom). Piscataway: IEEE Press, 2022: 83-88.
 - [16] SILVA D V, RAFAEL G R. Ontology for data integration in honeynet[J]. Journal of Positive School Psychology, 2022, 6(8): 10625-10637.
 - [17] PITTMAN J M, ALAEE S. A green scheduling algorithm for cloud-based honeynets[J]. Frontiers in Sustainability, 2023(3): 1048606.
 - [18] TAO J, CHEN A, LIU K, et al. Recommendation method of honeynet trapping component based on LSTM[C]//Proceedings of the 2021 IEEE Intl Conf on Dependable, Autonomic and Secure Computing, Intl Conf on Pervasive Intelligence and Computing, Intl Conf on Cloud and Big Data Computing, Intl Conf on Cyber Science and Technology Congress (DASC/PiCom/CB-DCom/CyberSciTech). Piscataway: IEEE Press, 2021: 952-957.
 - [19] SHENG C, YAO Y, LI D B, et al. Honeyeye: a network traffic collection framework for distributed ICS honeynets[C]//Proceedings of the 2020 IEEE Intl Conf on Parallel & Distributed Processing with Applications, Big Data & Cloud Computing, Sustainable Computing & Communications, Social Computing & Networking (ISPA/BDCLOUD/SocialCom/SustainCom). Piscataway: IEEE Press, 2020: 466-473.
 - [20] HOFFMAN F. Industrial Internet of things vulnerabilities and threats: what stakeholders need to consider[J]. Issues in Information Systems, 2019, 20(1): 119-133.
 - [21] YU T X, ZHANG C Y, XIN Y. Game-theoretical cyber deception strategy generation based on honeynet and intrusion prediction[C]//Proc SPIE 12609, International Conference on Computer Application and Information Security (ICCAIS 2022), 2023, 12609: 308-316.
 - [22] PETRE C A, KORODI A. Honeypot inside an OPC UA wrapper for water pumping stations[C]//Proceedings of the 2019 22nd International Conference on Control Systems and Computer Science (CSCS). Piscataway: IEEE Press, 2019: 72-77.
 - [23] ZHANG W, ZHANG B, ZHOU Y, et al. An IoT honeynet based on multiport honeypots for capturing IoT attacks[J]. IEEE Internet of Things Journal, 2020(5).
 - [24] CAMPOS M, GOMES E, MACHADO R. Sensors for detection of cyber threats on industrial environment using a high interaction ICS/SCADA honeynet[C]//Proceedings of the 2022 IEEE International Workshop on Metrology for Industry 4.0 & IoT (MetroInd4.0&IoT). Piscataway: IEEE Press, 2022: 1-5.
 - [25] TAN L, YU K P, MING F P, et al. Secure and resilient artificial intelligence of things: a honeynet approach for threat detection and situational awareness[J]. IEEE Consumer Electronics Magazine, 2022, 11(3): 69-78.
 - [26] SHAN Y, YAO Y, ZHAO T, et al. NeuPot: a neural network-based honeypot for detecting cyber threats in industrial control systems[J]. IEEE Transactions on Industrial Informatics, 2023, 19(10): 10512-10522.
 - [27] LUCCHESI M, LUPIA F, MERRO M, et al. HoneyICS: a high-interaction physics-aware honeynet for industrial control systems[C]//Proceedings of the 18th International Conference on Availability, Reliability and Security. New York: ACM, 2023: 1-10.
 - [28] JAVADPOUR A, JA'FARI F, TALEB T, et al. A mathematical model for analyzing honeynets and their cyber deception techniques[C]//Proceedings of the 2023 27th International Conference on Engineering of Complex Computer Systems (ICECCS). Piscataway: IEEE Press, 2023: 81-88.
 - [29] SIBI CHAKKARAVARTHY S, SANGEETHA D, CRUZ M V, et al. Design of intrusion detection honeypot using social leopard algorithm to detect IoT ransomware attacks[J]. IEEE Access, 2020, 8: 169944-169956.
 - [30] JAVADPOUR A, JA'FARI F, TALEB T, et al. A comprehensive survey on cyber deception techniques to improve honeypot performance[J]. Computers & Security, 2024: 103792-103831.
 - [31] ZHANG W Z, ZHANG B, ZHOU Y, et al. An IoT honeynet based on multiport honeypots for capturing IoT attacks[J]. IEEE Internet of Things Journal, 2020, 7(5): 3991-3999.
 - [32] FRANCO J, ARIS A, CANBERK B, et al. A survey of honeypots and honeynets for Internet of things, industrial Internet of things, and cyber-physical systems[J]. IEEE Communications Surveys & Tutorials, 2021, 23(4): 2351-2383.
 - [33] FU Q, YAO Y, SHENG C, et al. Interplay between malware epidemics and honeynet potency in industrial control system network[J]. IEEE Access, 2020, 8: 81582-81593.
 - [34] CHEN H S, CHO J H, XU S H. Quantifying the security effectiveness of firewalls and DMZs[C]//Proceedings of the 5th An-

- nual Symposium and Bootcamp on Hot Topics in the Science of Security. New York: ACM, 2018: 1-11.
- [35] BEHAM M, VLAD M, REISER H P. Intrusion detection and honeypots in nested virtualization environments[C]//Proceedings of the 2013 43rd Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN). Piscataway: IEEE Press, 2013: 1-6.
- [36] KYRIAKOU A, SKLAVOS N. Container-based honeypot deployment for the analysis of malicious activity[C]//Proceedings of the 2018 Global Information Infrastructure and Networking Symposium (GIIS). Piscataway: IEEE Press, 2018: 1-4.
- [37] MASHIMA D, KOK D, LIN W, et al. On design and enhancement of smart grid honeypot system for practical collection of threat intelligence[C]//13th USENIX Workshop on Cyber Security Experimentation and Test (CSET 20). 2020: 1-9.
- [38] MAESSCHALCK S, GIOTSAS V, RACE N. World wide ics honeypots: a study into the deployment of conpot honeypots[C]//Industrial Control System Security Workshop. 2021: 1-10.
- [39] CHOWDHURY S Y, DUDLEY B, SUN R M. The case for virtual PLC-enabled honeypot design[C]//Proceedings of the 2023 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW). Piscataway: IEEE Press, 2023: 351-357.
- [40] YANG X Y, YUAN J, YANG H, et al. A highly interactive honeypot-based approach to network threat management[J]. Future Internet, 2023, 15(4): 127.
- [41] POTHAMSETTY V, FRANZ M. Scada honeynet project: building honeypots for industrial networks[J]. SCADA Honeynet Project, 2005, 15.
- [42] HANEY M, PAPA M. A framework for the design and deployment of a SCADA honeynet[C]//Proceedings of the 9th Annual Cyber and Information Security Research Conference on-CISR '14. New York: ACM, 2014: 121-124.
- [43] VASILOMANOLAKIS E, SRINIVASA S, CORDERO C G, et al. Multi-stage attack detection and signature generation with ICS honeypots[C]//Proceedings of the NOMS 2016-2016 IEEE/IFIP Network Operations and Management Symposium. Piscataway: IEEE Press, 2016: 1227-1232.
- [44] SINIOGLOU I, EFSTATHOPOULOS G, PLIATSIOS D, et al. NeuralPot: an industrial honeypot implementation based on deep neural networks[C]//Proceedings of the 2020 IEEE Symposium on Computers and Communications (ISCC). Piscataway: IEEE Press, 2020: 1-7.
- [45] LAU S, KLICK J, ARNDT S, et al. POSTER: towards highly interactive honeypots for industrial control systems[C]//Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security. New York: ACM, 2016: 1823-1825.
- [46] XIAO F, CHEN E H, XU Q. S7commTrace: a high interactive honeypot for industrial control system based on S7 protocol[C]//Proceedings of International Conference on Information and Communications Security. Cham: Springer, 2018: 412-423.
- [47] DING C P, ZHAI J T, DAI Y W. An improved ICS honeypot based on SNAP7 and IMUNES[C]//Proceedings of International Conference on Cloud Computing and Security. Cham: Springer, 2018: 303-313.
- [48] REDWOOD O, LAWRENCE J, BURMESTER M. A symbolic honeynet framework for SCADA system threat intelligence[C]//Proceedings of International Conference on Critical Infrastructure Protection. Cham: Springer, 2015: 103-118.
- [49] GRAMMATIKIS P R, SARIGIANNIDIS P, DALAMAGKAS C, et al. SDN-based resilient smart grid: the SDN-microSENSE architecture[J]. Digital, 2021, 1(4): 173-187.
- [50] FERRETTI P, POGLIANI M, ZANERO S. Characterizing background noise in ICS traffic through a set of low interaction honeypots [C]//Proceedings of the ACM Workshop on Cyber-Physical Systems Security & Privacy-CPS-SPC'19. New York: ACM, 2019: 51-61.
- [51] BERNIERI G, CONTI M, PASCUCCI F. MimePot: a model-based honeypot for industrial control networks[C]//Proceedings of the 2019 IEEE International Conference on Systems, Man and Cybernetics (SMC). Piscataway: IEEE Press, 2019: 433-438.
- [52] DU M, WANG K. An SDN-enabled pseudo-honeypot strategy for distributed denial of service attacks in industrial Internet of things[J]. IEEE Transactions on Industrial Informatics, 2020, 16(1): 648-657.
- [53] ZARCA A M, BERNABE J B, SKARMETA A, et al. Virtual IoT honeynets to mitigate cyberattacks in SDN/NFV-enabled IoT networks[J]. IEEE Journal on Selected Areas in Communications, 2020, 38(6): 1262-1277.
- [54] ZHENG M J, MA Y F, WU B, et al. A dynamic deceptive honeynet system with a hybrid of virtual and real devices[C]//Proceedings of the 2022 5th International Conference on Computing and Big Data (ICCBD). Piscataway: IEEE Press, 2022: 113-117.
- [55] TRIANTOPOULOU S, PAPANIKAS D, KOTZANIKOLAOU P. An experimental analysis of current DDoS attacks based on a provider edge router honeynet[C]//Proceedings of the 2019 10th International Conference on Information, Intelligence, Systems and Applications (IISA). Piscataway: IEEE Press, 2019: 1-5.
- [56] BOUKELA L, ZHANG G X, BOUZEFRANE S, et al. An outlier ensemble for unsupervised anomaly detection in honeypots data[J]. Intelligent Data Analysis, 2020, 24(4): 743-758.
- [57] TOK M S, DENER M, DEMIRCI M. Processing honeypot logs with big data and data visualization via hadoop- power BI integration[C]//Proceedings of the 2022 15th International Conference on Information Security and Cryptography (ISCTURKEY). Piscataway: IEEE Press, 2022: 49-54.
- [58] MUDGAL A, BHATIA S. Big data enabled intrusion detection with honeypot intelligence system on apache flink (BDE-IDHIS) [C]//Proceedings of the 2023 14th International Conference on Computing Communication and Networking Technologies (ICCCNT). Piscataway: IEEE Press, 2023: 1-6.
- [59] QI Y L, JIANG R, JIA Y, et al. Attack analysis framework for cyber-attack and defense test platform[J]. Electronics, 2020, 9(9): 1413.
- [60] HOBERT K, LIM C, BUDIARTO E. Enhancing cyber attribution through behavior similarity detection on linux shell honeypots with ATT&CK framework[C]//Proceedings of the 2023 IEEE International Conference on Cryptography, Informatics, and Cybersecurity (ICoCICs). Piscataway: IEEE Press, 2023: 139-144.

[作者简介]



陈曦（1987-），男，山东淄博人，北京大学博士生、中国电子信息产业发展研究院高级工程师，主要研究方向为工业控制系统软硬件质量、安全测评。



林昕（1988-），男，天津人，中国软件评测中心（工业和信息化部软件与集成电路促进中心）高级工程师，主要研究方向为工业控制系统软硬件质量与安全测评。



姜亚光（1985-），女，内蒙古呼伦贝尔人，中国软件评测中心（工业和信息化部软件与集成电路促进中心）高级工程师，主要研究方向为工业控制系统软硬件质量与安全测评。



周文（1974-），男，四川宣汉人，中国民用航空局高级工程师，主要研究方向为网络安全与数字化。