

工业控制系统安全态势感知技术研究

周 明^{1,2}, 吕世超^{1,2}, 游建舟^{1,2}, 朱红松^{1,2}, 石志强^{1,2}, 孙利民^{1,2}

¹中国科学院信息工程研究所 物联网信息安全技术北京市重点实验室 北京 中国 100093

²中国科学院大学 网络空间安全学院 北京 中国 100049

摘要 工业控制系统(简称工控)是国家关键基础设施的核心,越来越多的工作开始关注工控系统安全。然而,这些工作的实际应用场景并不统一,因此他们取得的成果无法相互借鉴。为了解决这个问题,在深入研究这些安全技术的基础上,我们提出了工控系统安全态势感知(Situational Awareness for Industrial Control Systems Security, SA-ICSS)框架,该框架由态势觉察、态势理解和态势投射三个阶段构成。在态势觉察阶段,我们首先利用网络测绘和脆弱性发现技术获取完善的目标系统环境要素,如网络拓扑和漏洞信息;其次,我们将入侵检测和入侵诱捕等5种设备部署在目标系统中,以便从控制系统中捕获所有的可疑活动。在态势理解阶段,我们首先基于结构化威胁信息表达(Structured Threat Information Expression, STIX)标准对目标系统进行本体建模,构建了控制任务间的依赖关系以及控制任务与运行设备的映射关系;其次,自动化推理引擎通过学习分析师推理技术,从可疑活动中识别出攻击意图以及目标系统可能受到的影响。在态势投射阶段,我们首先利用攻击图、贝叶斯网络和马尔科夫模型从可疑活动中构建攻击模型;其次,我们利用现有的威胁评估技术从攻击模型中预测可能发生的攻击事件、可能被感染的设备以及可能存在的零日漏洞。我们阐述了 SA-ICSS 各个阶段的任务范围,并对其中的关键技术进行了分析与总结。最后,我们还探讨了 SA-ICSS 待解决的若干问题。

关键词 工业控制系统; 安全态势感知; 本体模型; 攻击意图; 影响评估; 威胁预测

中图法分类号 TP309.2 DOI号 10.19363/J.cnki.cn10-1380/tn.2022.03.07

A Comprehensive Survey of Security Situational Awareness on Industrial Control Systems

ZHOU Ming^{1,2}, LV Shichao^{1,2}, YOU Jianzhou^{1,2}, ZHU Hongsong^{1,2}, SHI Zhiqiang^{1,2}, SUN Limin^{1,2}

¹Beijing Key Laboratory of IoT Information Security Technology, Institute of Information Engineering, Chinese Academy of Sciences, Beijing 100093, China

²School of Cyber Security, University of Chinese Academy of Sciences, Beijing 100049, China

Abstract Industrial Control Systems (ICS) are the core part of the state critical infrastructure, and more and more works are focusing on the ICS security. However, the results of these works cannot apply to each other since their application situations are not all the same. To solve this problem, we propose a Situational Awareness for Industrial Control Systems Security (SA-ICSS) framework that integrates many security techniques proposed in recent years, and the framework involves three stages: situational perception, situational comprehension, and situational projection. In situational perception stage, we first obtain the full environmental elements from the target control system by using the network scanning and vulnerability discovery techniques, such as network topology and vulnerability information; then we deploy five kinds of security devices such as intrusion detection and intrusion deception systems in the target control system, these devices help us collect potential malicious activities. In situational comprehension stage, we first construct an ontology model for the target control system based on the Structured Threat Information Expression (STIX) standards, which involves the dependency relationship among control tasks and the mapping relationship between control tasks and their corresponding devices; then an automatic reason engine is used to learn reason rules from the security analyzers, and the engine can automatically identify the attack intention and the possible impacts against the target control system. In situational projection stage, we first construct an attack model based on the above malicious activities by using three attack modeling techniques including attack graph, Bayesian attack graph, and Markov model; Once the attack model is built, we use the off-the-shelf threat evaluation techniques to predict the possible results appearing in the future, such as attack events, infected devices, and “0-day” vulnerabilities. In this paper, we elaborate the task scope at each stage of the SA-ICSS and summary the key technologies among these stages. Finally, we discuss five open problems that have not been solved on the SA-ICSS.

Key words industrial control systems; security situational awareness; ontology model; attack intent; impact assessment; threat prediction

通信作者: 吕世超, 博士, 高级工程师, Email: lvshichao@iie.ac.cn。

本课题得到国家重点研发计划(No. 2018YFC1201102), 国家自然科学基金重点项目(No. U1766215), 国家自然科学基金项目(No. 61702506)资助。

收稿日期: 2019-08-19; 修改日期: 2019-10-28; 定稿日期: 2022-01-07

1 引言

工业控制系统(以下简称工控系统)由各种自动化组件和实时数据采集、监测的过程控制组件共同构成,用于监测和控制工业生产过程,确保工业设备正常运行。工控系统包括数据采集与监控系统(Supervisory Control and Data Acquisition, SCADA)、分布式控制系统(Distributed Control Systems, DCS)、可编程逻辑控制器(Programmable Logic Controller, PLC)、远程终端(Remote Terminal Unit, RTU)和人机交互界面(Human Machine Interface, HMI),它是电力、燃气、石化等国家关键基础设施的核心。

自 2010 年伊朗核电站遭到 Stuxnet 病毒感染导致离心机损毁以来^[1],针对工控系统的破坏性攻击被大量曝光,如 2014 年德国钢铁厂遭到鱼叉式网络钓鱼导致熔炉爆炸^[2],2015 年乌克兰电网遭到 BlackEnergy 病毒感染导致居民区停电^[3],越来越多的人相信对工业控制系统的入侵是完全可能发生的。2019 年委内瑞拉发生全国范围的大面积停电事故^[4],但调查组难以深入实地进行观察,也无恶意代码样本、异常日志、系统镜像等取证数据,因此无法判断该事故的真实原因。

亟需全面地研究工控系统安全技术,构建稳定、安全、实用的工控安全态势感知系统。为保护工控系统安全,分析师必须理解工控环境中人、网络、物理之间大量的相互作用。工控系统拓扑结构复杂多变,噪音信号突出,各种威胁快速演变,事故发生的速度超出人类处理的极限。当前出现的众多检测和防御技术各自为战,远未达到态势感知的要求。虽然感知数据来源丰富,但缺乏学习这些数据语义的技术。态势感知不仅涉及入侵检测等安全技术,还受到认知等多个学科发展的制约。高度自动化的检测和防御工具的输出不易被分析师理解,限制了分析师将新事件、新假设、新处理动作载入上述自动化机制的能力。以上诸多因素为工控系统安全态势感知提出了严峻挑战。近年来,工控系统安全态势感知技术不断取得新进展。Urbina 等人^[5]以单位时间内未被检测的攻击对传感器产生的最大偏移为度量标准,检测将攻击影响控制在阈值以下的隐蔽攻击。Abbasi 等人^[6]利用 PLC 每个周期消耗的 CPU 时钟数量检测 PLC 控制流劫持攻击。Vasilomanolakis 等人^[7]将蜜罐捕获的攻击特征应用到入侵检测系统中,发现了工控系统来自同源不同协议的多步 APT 攻击。Kriaa 等人^[8]利用条件依赖、相互强化、对抗和无关四种依赖关系来解释与理解工控系统物理安全和网络安全

之间的关系。Zhong 等人^[9]研发了采集分析师认知轨迹的工具 ARSCA。Yao 等人^[10]利用 PLC-PC 蠕虫传播模型预测蠕虫在 PC 和 PLC 之间的传播情况。Teixeira 等人^[11]利用先验知识、内部资源和攻击策略为攻击者建模,并从威胁可能性和威胁影响两方面量化工控系统安全风险。

目前国内外缺少对工控系统安全态势感知技术的综述性工作。本文围绕如何形成工控系统安全态势感知这个主题,讨论分析师形成该能力需要哪些关键技术支持,并分析、总结了相关研究的工作进展(图 1)。本文的主要贡献如下:

(1) 分析和总结了工控系统安全态势感知相关的研究工作,并在此基础上提出了更为具体、合理的工控系统安全态势感知模型,进一步明确了它的研究目标。

(2) 讨论了工控系统安全态势感知在态势觉察、态势理解和态势投射三个阶段的任务范围,并对相关的研究内容进行了分类讨论。

(3) 讨论了工控系统安全态势感知待解决的若干问题,进一步指出工控系统安全态势感知下一步的研究重点。

本文的组织结构如下:第 2 节提出了工控安全态势感知框架;第 3 节~第 5 节分别从态势觉察、态势理解、态势投射这三个方面阐述工控系统安全态势感知的研究内容和关键技术;第 6 节讨论了工控系统安全态势感知待解决的问题;第 7 节对全文进行了总结。

2 工控系统安全态势感知模型

工控系统安全态势感知研究的最终目标是:设计能够获得自我意识的系统,并利用这种意识来实现工控系统的自动保护和修复能力,而不需要人员参与感知过程的具体工作。Endsley^[12]提出了被广泛引用的态势感知定义,该定义的描述是:“在一定的时间和空间内观察环境中的元素,理解这些元素的意义,并预测这些元素在不久的将来的状态。”基于该定义,态势感知由觉察(perception)、理解(comprehension)和投射(projection)三层构成。本文将 Endsley 的态势感知模型应用到工控系统安全领域,我们提出了工控系统安全态势感知模型(图 2)。该模型包括态势觉察、态势理解和态势投射三个阶段,工控系统监测与检测数据以及工控业务所运行的环境是态势觉察的输入,其输出的觉察结果作为态势理解和态势投射的输入,态势理解和态势投射的输出即整个工控系统态势感知模型的输出。态势觉察阶



图 1 工控系统安全态势感知关键技术

Figure 1 Key technologies of situational awareness for industrial control systems security

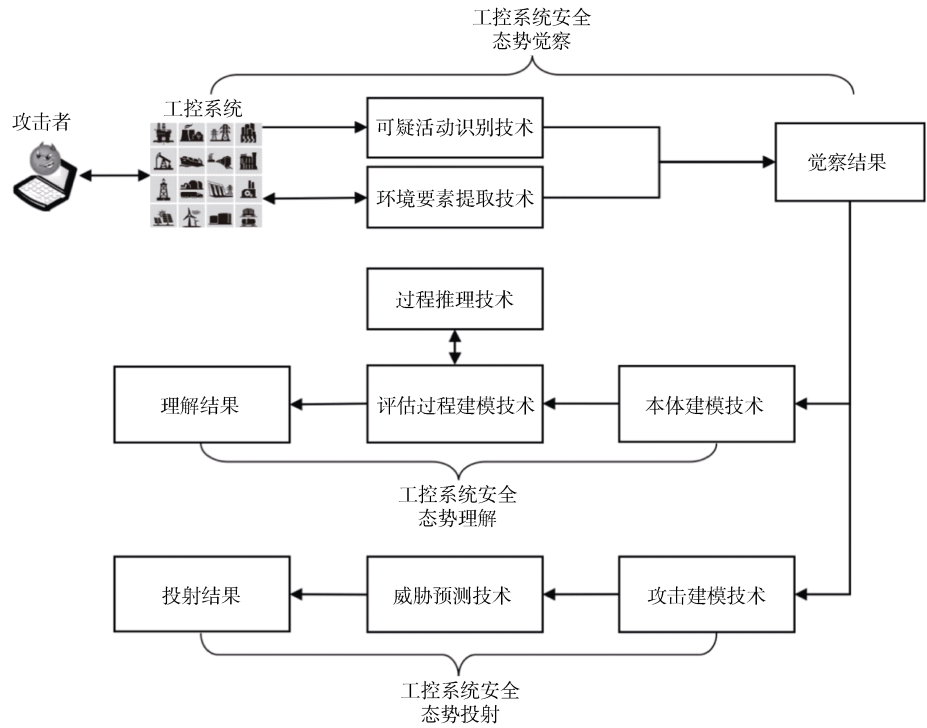


图 2 工控系统安全态势感知模型

Figure 2 Model of situational awareness for industrial control systems security

段的任务是识别工控系统的可疑活动, 以及这些活动出现时所依赖的网络拓扑等环境要素。态势理解阶段的任务是工控系统业务构建本体模型, 并利用过程推理技术从态势觉察结果中理解攻击者意图, 评估系统可靠性以及工作任务受到的影响。态势投射阶段的任务是基于态势觉察的结果为攻击者行为建模, 并利用该攻击模型预测威胁事件。

3 工控系统安全态势觉察

工控系统安全态势觉察阶段的基本任务是对目标系统中的活动以及该系统所运行环境中显著信息的辨识, 回答“那是什么”的问题。如图 3 所示, 在工控系统安全态势觉察阶段, 入侵检测、入侵诱捕、

故障检测、防火墙拦截、物理域与信息域依赖关系检测、网络拓扑测绘、脆弱性发现等技术为态势感知提供丰富的数据来源。前 5 种技术从工控系统识别恶意攻击和偶然故障等可疑活动, 后 2 种技术从工控系统提取网络拓扑和脆弱性等环境要素。

3.1 可疑活动识别技术

近年来, 出现了大量工控可疑活动识别技术, 如入侵检测、入侵诱捕、故障检测、物理域与信息域依赖关系检测和防火墙拦截。这些技术主要应用于事后取证分析, 推断攻击者意图(4.3 节)。可疑活动识别技术主要采用被动监测方式发现工控系统恶意攻击活动和偶然故障活动。下面介绍这些技术的取证类型和工作原理。

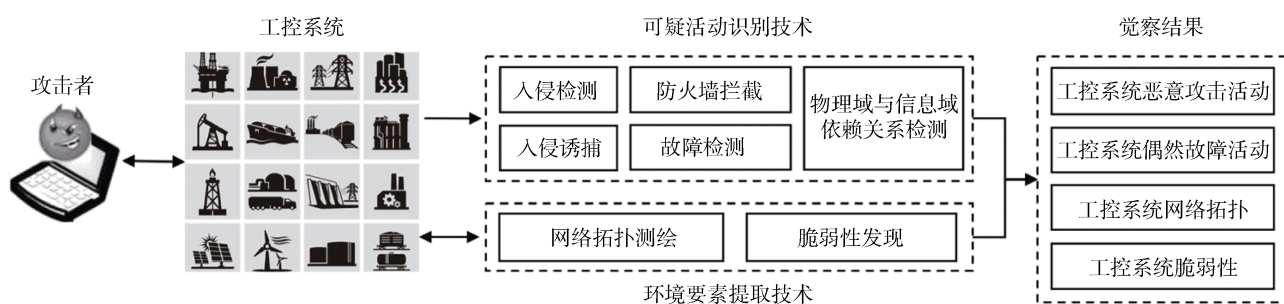


图 3 工控系统安全态势觉察模型

Figure 3 Perception model of situational awareness for industrial control systems security

3.1.1 入侵检测

根据数据来源, 我们将工控入侵检测技术分为基于网络流量、基于物理过程和基于侧信道 3 种类型。工业设备种类繁多, 跨越了从物理执行层、控制层、监视层等多个层次, 造成了工业网络协议众多, 既有 Profibus、Interbus 这样的总线协议, 也有 Modbus、Siemens S7、DNP3、OPC、CIP 这样的以太网协议^[13]。

基于网络流量的工控入侵检测多针对上述协议, 方法主要有基于协议载荷和基于流量外观两种。基于协议载荷指将工业协议中的数据载荷作为检测特征, 利用机器学习、数据挖掘等方法发现载荷中的恶意攻击^[14]。基于流量外观指将数据包大小、数据包时间间隔、会话时间、丢弃数据包数量等作为检测特征, 利用机器学习、数据挖掘算法发现载荷中的恶意攻击^[17-18]。许多工业网络协议是私有的, 即没有公开协议信息, 这时候需要利用协议逆向技术解析协议字段、字段含义及其数据类型。若无法通过协议逆向解析协议, 可通过流量外观检测工业网络载荷中的攻击。

基于物理过程的工控入侵检测系统的输入是传

感器、执行器等控制现场端测量值, 这些测量值可来自历史数据库, 也可直接来自传感器。基于业务过程的工控入侵检测方法主要有基于控制逻辑和基于过程状态, 控制逻辑指任务调度的时间序列和控制程序遵循的物理规律, 过程状态指监测变量的残差和临界状态。任务调度的时间序列方法通常利用控制程序任务调度的开始、结束时间作为特征, 检测控制程序中异常的调度任务^[19]; 工业领域的控制程序通常是为了完成一系列控制过程而设计的, 因此其必然满足这些控制过程的物理规律, 最常用到的物理规律是系统动力学^[22]和过程行为约束^[16]。过程状态的变量残差通常利用仪表的直接观测值与测量值的差值作为特征, 检测测量值篡改类攻击, 最常使用的方法是排列熵累积和算法^[5]; 过程状态的临界状态通常利用系统从正常状态到异常状态的临界点作为特征, 检测控制命令篡改类攻击, 最常使用的方法是有限确定自动机^[28]和数据挖掘算法^[29]。

基于侧信道的工控入侵检测系统的输入是电磁信号、能耗、PLC 时钟数量、噪音指纹、旁路检测等设备端物理信息。PLC 电路在执行控制程序时会发射电磁信号, 可利用该信号检测控制流完整性攻

击^[30]。传感器和执行器会消耗一定的电能,可利用该能耗检测控制器数据完整性攻击^[31]。PLC 每个任务周期消耗的 CPU 时钟数量不同,可利用这个特点检测 PLC 控制流劫持攻击^[6]。传感器存在制造瑕疵、独有的物理过程等噪音指纹,可利用该指纹检测传感器数据完整性攻击^[32]。可直接从传感器和执行器收集数据,而非从控制器、网络交换机、历史数据库等监控层设备收集数据,防止监测数据被篡改^[33]。

3.1.2 入侵诱捕

工控系统对外部操作很敏感,通过在工控系统的关键位置部署入侵诱捕装置(即蜜罐),可在一定程度上扩展态势觉察的深度。该装置可通过多种诱骗策略吸引攻击者,并以深度交互的方式获取详细的攻击步骤。

最著名的通用蜜罐是 Honeyd,许多工作将 Honeyd 扩展为适应工控场景的蜜罐。Vollmer 等人^[34]利用 Etterap 工具被动地识别工控网络资产,并将资产的 IP 地址、MAC 地址和端口使用等信息输出到 Honeyd 蜜罐,通过该方法构建了 12 种工控网络堆栈特征蜜罐。其中 8 种蜜罐成功欺骗了 Nmap 扫描工具,实验表明工控蜜罐的仿真度与是否来自非 IP 流量、是否有操作系统数据库支持、是否存在关键信息缺失、是否具有良好的程序输出等因素有关。Winn 等人^[35]研发了基于 Honeyd 的工控蜜罐代理,该代理从真实 PLC 中获取 IP 地址、MAC 地址、端口信息、操作系统指纹等配置信息,并以 Raspberry Pi 为载体生成多个虚拟 PLC 蜜罐。

常见的开源工控蜜罐是 CryPLH^[36]和 Conpot^[37]。CryPLH 在基于 Linux 的虚拟机中集成了一些 PLC 服务。Conpot 集成了 Modbus、Siemens S7、BACNet 等多种工业网络协议,并可通过修改配置文件的方式仿真品牌、型号、组件名称等具体控制器信息,提高其仿真程度。Irvine 等人^[38]利用 HoneyPhy 研发了一个机器人物理感知蜜罐,该蜜罐模拟了多个不安全操作,并通过与攻击者的交互构建攻击者模型。Vasilomanolakis 等人^[7]将蜜罐捕获的攻击特征应用到入侵检测系统,发现了工控系统中来自同源不同协议的多步 APT 攻击。为捕获工控系统高级恶意软件,Rrushi 等人^[39]在控制器蜜罐的 OS 内核载入网卡、磁盘、固态驱动器、I/O 面板等多个虚拟功能,并利用动态欺骗策略诱导恶意程序进入蜜罐陷阱。

3.1.3 故障检测

尽管工控系统在设计时考虑到可靠性,但鉴于有些工控系统运行在高温、嘈杂的恶劣环境,且实际业务流程存在物料短缺、断电等突发情况,工控系统

会发生偶然性故障,分析师根据故障排除恶意攻击,从而将注意力转移到更紧急/重要的可疑活动。

Fang 等人^[40]总结了工控网络故障诊断的主要思路,提出了基于信息调度的工控网络故障诊断的基本原则,并重点介绍了基于简化时滞系统模型,以及长时延线性和非线性近似 T-S 模糊模型等工控网络故障诊断方法。Gu 等人^[41]通过选择性检测控制流子集的方法解决运行时开销与故障检测覆盖率之间的矛盾。恶劣的工控现场环境会导致 RTU 处理器产生瞬时控制流错误,Rajabpour 等人^[42]利用控制流校验技术检测 RTU 控制流错误。发现电网所有意外故障是不现实的,Santos 等人^[43]将电网故障选择转化为组合优化问题,并利用两个改进的遗传算法发现较严重的电网故障。工控系统的监视数据稀疏,且缺乏描述严重故障的训练数据,因此以前的方法不能持续、可信、稳定地监视系统故障。Weimer 等人^[44]以工控系统中的不变参数为特征,利用二元假设检验(binary hypothesis testing)技术检测工控系统故障。在动态网络系统、线性时不变系统和混合系统 3 种实际 CPS 场景实验了上述方法,结果表明系统变化和未知攻击事件几乎不影响 PAIN 监视器的性能。Pan 等人^[45]通过融合同步向量数据、网络安全日志和供电管理系统日志,并利用通用路径算法检测电力系统故障、干扰和网络攻击。

3.1.4 物理域与信息域依赖关系检测

与传统 IT 系统相比,工控系统的态势理解不仅需要考虑恶意攻击,还需要考虑设计时错误和运行时故障^[46]。实际上,近些年来工业界和学术界普遍认为工控系统安全需要将物理安全和网络安全结合起来,并找到它们之间的依赖关系。Kriaa 等人^[8]分析比较了工控物理安全和网络安全之间的 4 种相互依赖关系,即条件依赖(conditional dependency)、相互强化(mutual reinforcement)、对抗(antagonism)和无关(independency)。其中,条件依赖指网络安全是物理安全需求的先决条件,反之亦然;互相强化指满足物理安全需求或物理安全措施有助于提高网络安全,反之亦然,利于实现资源优化和降低成本;对抗指物理安全需求或物理安全措施与网络安全需求或网络安全措施相互冲突,此种情况优先考虑物理安全;无关指物理安全与网络安全间没有关系。Zhou 等人^[47]发现工控系统控制环路的控制节点之间遵循一致性和互补性规律,并指出当控制环路中的某些控制器节点被攻击者破坏,这些规律也会被破坏,防御者可利用该原理检测工控系统攻击。

基于 ISA84 和 ISA99 标准,Sabaliauskaite 等人^[48]

提出了 6 步工控系统物理安全与网络安全分析模型。该模型从系统功能、系统结构、系统故障、物理安全措施、网络攻击及其安全措施等 6 个维度分析工控系统安全性。该模型融合了工控物理安全和网络安全的生命周期, 同时考虑了物理安全中的故障树及其安全策略、网络安全中的攻击树及其对策。Castellanos 等人^[49]从 PLC 代码中自动提取物理信息域的依赖关系, 并基于这些依赖关系构建整个工控系统的数据流图, 最后利用可达性分析算法帮助分析师从数据流图中发现可被利用的攻击点。Adepu 等人^[50]利用状态条件图(State Condition Graphs, SCGs)表示工控系统物理组件和网络组件的关系, 并通过多智能体(Agent)框架分析控制流中传感器、执行器和网络组件之间的交互, 辅助分析师了解工控系统在攻击后的响应状态。

3.1.5 防火墙拦截

入侵检测技术的主要功能是检测, 而防火墙技术是拦截。实际上, 被防火墙拦截的操作对分析师具有重要的参考价值。现有的防御手段很难抵御 APT 攻击, 但在持续性的探测和攻击过程中, APT 初期的一些操作会被防火墙拦截, 若分析师觉察到这些告警, 能极大地提高对入侵者的攻击意图推测能力。基于关键状态距离, Fovino 等人^[51]提出了一种监视、分析和过滤 SCADA 主从设备间命令数据包中的防火墙, 该防火墙仅过滤会引起控制系统到达危险状态的数据包, 因此误报率较低。

Li 等人^[52]提出了一种实用的 SCADA 防火墙方案, 该方案包括 3 个组件: (1) 专有工业协议扩展算法 PIPEA, 该算法可从专有协议中提取检测规则; (2) 基于上述检测规则, 利用综合数据包检测技术从工业协议的功能码、操作目标与地址、子功能码等特定用途字段发现恶意载荷; (3) 提出了无序检测算法(out-of-sequence detection algorithm, OSDA)拦截异常的工控操作。

3.2 环境要素提取技术

除了可疑活动, 态势觉察阶段还应该为态势系统提供这些可疑活动的上下文信息, 如网络拓扑和脆弱性信息。网络拓扑技术主要采用主动扫描方式不断更新工控系统的网络拓扑结构, 脆弱性发现技术主要采用主动扫描方式不断更新工控系统资产和服务的漏洞信息。下面分别介绍这两种技术。

3.2.1 网络拓扑测绘

网络测绘技术是态势觉察阶段的核心技术, 网络测绘的基本任务是对工控网络中的资产、服务、任务及其依赖关系进行动态建模。要实现动态建模

需首先获取工控网络中的资产、服务及其依赖关系等指纹信息, 但工控领域并无成熟的技术可用, 因此, Caselli 等人^[53]讨论了将 IT 系统指纹识别技术推广到工控系统的可能性, 指出工控系统需要考虑的具体特征及其在指纹识别时面临的挑战, 并提出了工控指纹识别参考模型。

虽然还没有公开文献专门研究企业级工控系统指纹识别技术, 但针对 Internet 上工控系统的网络测绘技术已经较为成熟。文献[54]通过精心构造的 17 种工业网络协议数据包探测 Internet 上可公开访问的工控设备, 并利用蜜罐识别技术排除虚假的工控设备后, 在 20 h 内从全球近 37 亿的 IP 地址空间发现了 141008 个在线工控设备。Formby 等人^[55]提出了两种被动控制设备指纹识别方法, 第一种方法基于工控网络低延迟特征, 以网络请求的响应时间作为设备指纹; 第二种方法以工控设备的物理操作时间作为设备指纹。Mirian 等人^[56]利用 ZMap 工具从互联网上搜索运行 SCADA 系统的设备, 发现了 60000 个可公开访问的相关设备。

获取工控网络中资产、服务及其依赖关系的指纹信息后, 需结合具体业务流程, 对工控网络中的资产、服务及其依赖关系建模。Jakobson^[57]提出了网络空间地形概念, 以便对网络资产及其依赖关系、网络对象的漏洞和运行能力进行建模。工控网络由网络资产地形、软件资产地形和服务地形构成。网络资产由互联的网络硬件组成, 包括工业交换机、工业路由器、PLC、RTU、IED、SCADA 服务器、DCS 服务器、业务数据库等, 组件之间的连接关系表示网络资产地形的物理和逻辑拓扑结构。软件资产地形由操作系统、中间件和应用程序的不同软件构成, 并且定义了软件之间的依赖关系。服务地形描述了所有服务以及它们之间的依赖关系, 最常见的依赖关系是其他服务启动某个服务, 以及某个服务包含另一些服务。

3.2.2 脆弱性发现

态势理解阶段需进行系统可靠性和工作任务影响评估, 因此需首先通过脆弱性挖掘技术发现工控系统的漏洞, 并基于这些漏洞特征扫描目标系统是否存在上述工控漏洞, 扫描技术 3.2.1 节已经讨论过。脆弱性挖掘技术包括漏洞挖掘技术和漏洞关联技术, 前者通过模糊测试从工控组件中发现未知漏洞, 后者利用关联匹配技术从工控组件中发现相似的漏洞, 提高脆弱性挖掘的效率。研究工控漏洞关联技术的工作较少, 下面主要讨论工控漏洞挖掘技术。

2010 年前曝光的工控漏洞主要来自基于 PC 端

的 HMI 和工程师软件, 2010 年后越来越多的工控漏洞来自控制设备。通过逆向工程实验, Rouf 等人^[58]发现智能电表的自动抄表(Automatic Meter Reading, AMR)技术存在隐私性、完整性和认证等方面的漏洞。实验发现 ARM 仪表每隔 30 s 会通过不安全的无线链路广播其用电数据, 该漏洞可使攻击者监控邻近区域的数百个家庭用电情况, 进而推理出家里是否有人、主人的日常生活习惯等隐私。Shirani 等人^[59]提出了针对电网智能电子设备(intelligent electronic devices, IED)固件函数的漏洞挖掘方法。该方法首先基于一组异构特征过滤不相似函数, 其次基于上述特征的可执行路径进一步过滤不相似函数, 最后利用模糊图匹配技术识别漏洞函数, 该方法最大限度地降低了函数匹配的计算成本。Zhu 等人^[60]利用逆向工程技术挖掘工控固件漏洞, 首先采用 Find-string 算

法获取固件样本中字符串偏移量, 然后利用 Find-LDR 算法获取 LDR 指令的加载地址, 最后基于偏移量和 LDR 加载地址, 利用 DBMSSL 算法还原固件指令。

4 工控系统安全态势理解

工控系统安全态势理解阶段的基本任务是根据分析师的目标来确定目标系统中攻击活动及其运行环境等元素的意义或显著性, 对正在发生的恶意攻击事件形成更全面的整体理解, 回答“那意味着什么”的问题。如图 4 所示, 在工控系统安全态势理解阶段, 通过本体模型表示工控系统任务间依赖关系以及任务与资产映射关系, 并利用数据驱动型和认知驱动型两种技术推理态势的演变, 理解攻击者意图, 评估系统可靠性受到的影响以及任务流程受到的影响。

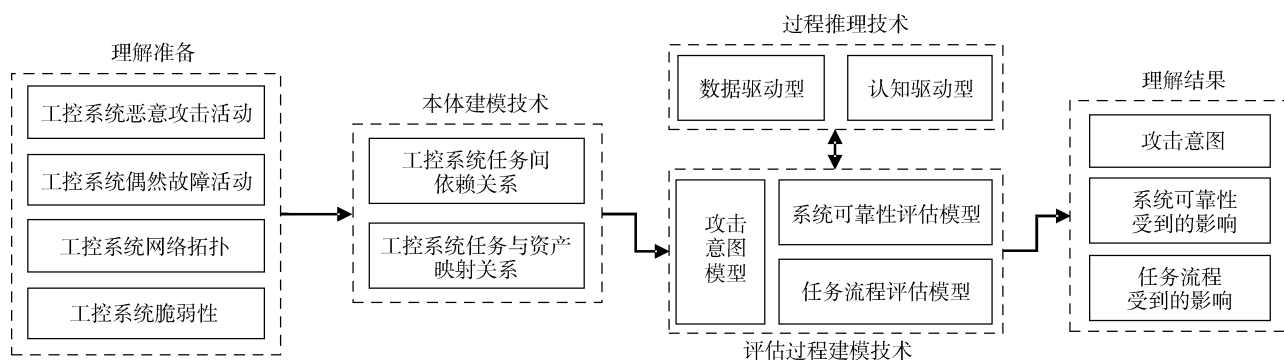


图 4 工控系统安全态势理解模型

Figure 4 Comprehension model of situational awareness for industrial control systems security

4.1 本体建模技术

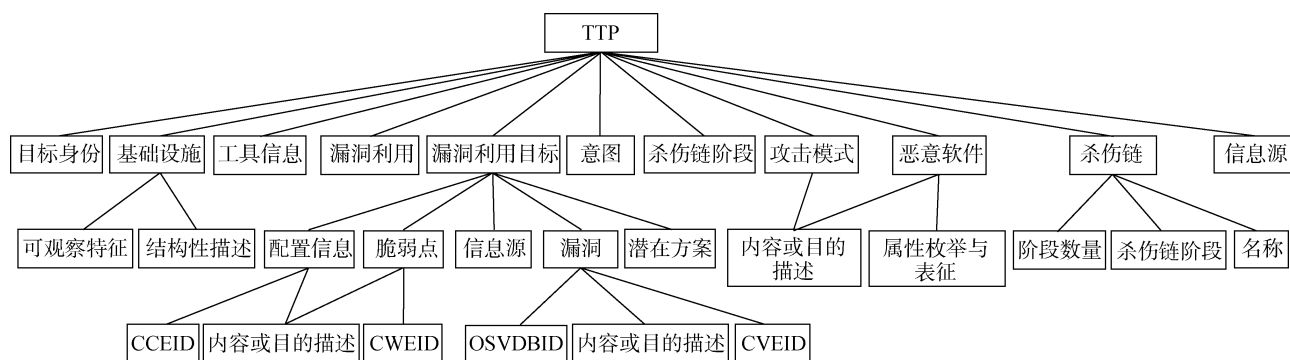
推理算法在态势理解方面具有关键作用, 推理算法能对大量态势觉察阶段发现的数据做出合理解释, 能推导出态势中的重要特征, 以辅助分析师迅速做出合理的决策。为了开展这种推导过程, 并使其输出能够被其它算法或分析师理解, 需要使用明确且唯一的术语, 以及术语间相互关系的词汇集, 用以表达推理算法的输入和输出, 这就需要构建具有清晰语义和标准定义的本体结构。

本体模型表示一种显示的、形式化的、机器可读的语义模型, 定义了与某一领域相关的类、类的实例、类间关系和数据属性^[61]。W3C(万维网联盟)组织产生了迄今为止得到最广泛应用的可互操作词汇集, 这些词汇集具有本体模型形式的语义体系, 并采用 Web 本体语言(Web Ontology Language, OWL)标准对本体模型进行编码。

目前得到各个组织和厂商广泛支持的是“结构化威胁信息表达”(Structured Threat Information eX

pression, STIX)标准, 该标准由 MITRE 公司管理和维护, 旨在实现态势信息的标准化描述、存储和共享。如图 5 所示, Ulicny 等人^[62]在其项目中展示了 STIX 本体模型的高阶描述。该模型的中心类是“战术、技术和规程”(Tactics Techniques Procedures, TTP), TTP 具有等多样化的子类, 其子类又可以被实例化为不同的对象属性。TTP 包括目标身份、基础设施、工具信息、漏洞利用、漏洞利用目标、意图、杀伤链阶段、攻击模式、恶意代码、杀伤链、信息源等子类。

业务本体模型是工控态势理解的基础, 为态势演化过程推理、攻击意图理解和工控业务影响评估提供结构化数据。工控业务由一系列工作任务协作完成, 因此需为每个任务以及任务间的依赖关系构建模型。工作任务树(4.4.2 节)利用树结构表示工作任务及其依赖关系, 该结构可通过任务影响关系图(4.4.2 节)评估工作任务受到的影响。这些工作任务需要特定的服务器、控制设备、服务和传感器等资产

图 5 STIX 本体模型的高阶描述^[62]Figure 5 High-level view of STIX ontology^[62]

支撑, 因此还需建立这些任务与其支撑资产之间的映射关系。虚拟地形^[63]使用图结构表示上述资产信息, 该结构利于建立从资产到服务、从服务到漏洞、从漏洞到可观察对象之间的映射关系。

目前来看, 大部分文献主要研究本体模型的形式化建模。根据工控系统的物理定律和逻辑状态变化情况, Rocchetto 等人^[64]对工控系统的物理交互过程进行形式化建模, 该模型的抽象水平被维持在较低水平, 因此包含了较为详细的状态信息, 以便进行后期的推理。Cheminod 等人^[65]提出了半自动化验证工业网络访问策略的方法, 该方法通过计算和比较“规范 S”和“实现 I”两个三元组(用户, 操作, 对象)来验证“谁被允许做什么”。该验证方法不仅能说明抽象的访问控制策略, 还能描述目标物理系统的细节。

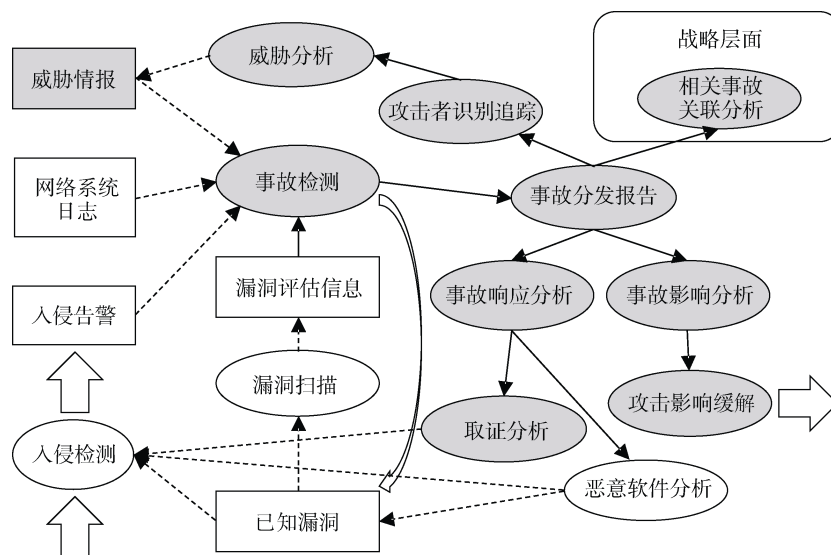
4.2 过程推理技术

基于 4.1 节工控系统业务本体模型, 利用自动化过程推理技术加快态势理解过程, 我们将过程推理

技术分为数据驱动型和认知驱动型。

4.2.1 数据驱动型

目前, 大部分工作的属于数据驱动型推理过程, 这部分工作的观点将态势理解过程划分为分类分流、事态升级、关联分析、威胁分析、漏洞评估、事件响应、取证分析和大局图景等八个阶段。Yen 等人^[66]总结了上述阶段之间的依赖关系, 这些依赖关系还突出了战术层面与战略层面分析过程的关系。如图 6 所示, 战术层面的分析任务包括入侵检测、漏洞扫描、事故检测、威胁分析、攻击者识别追踪、事故报告分发、事故响应分析、事故影响分析、取证分析、攻击影响缓解和恶意软件分析; 战略层面的分析指对相关安全事故的关联分析, 以便判断该事故是否是更大攻击事故的一部分。图 4 中的椭圆表示分析阶段, 矩形表示数据或信息, 实心椭圆表示通过手工分析, 空心椭圆表示计算机自动执行。

图 6 数据驱动型推理过程^[66]Figure 6 The data-driven reasoning process^[66]

除了 Yen 等人^[66]提出的数据驱动型推理过程, Coppolino 等人^[67]提出了另一种工控系统态势理解的思路, 即通过 SIEM 技术增强数据处理过程的方案, 该方案借助通用事件转换模块收集异构数据, 并采用弹性存储方法可靠地存储漏洞数据。

4.2.2 认知驱动型

认知驱动型指分析师执执行一系列动作和推理步骤的详细认知过程, 以及这些动作与推理步骤之间的关系。工控系统态势理解过程的概念模型以认知科学理论为基础, Zhong 等人^[9]将认知过程建立在动作(Action)、观察(Observation)和假设(Hypothesis) 3个关键的认知结构之上(即 A-O-H 模型)。如图 7 所示, 动作表示分析师对证据的探索活动, 观察表示分析师看到并认为具有相关性的数据或告警, 假设表示在某一确定情况下分析师的意识和假设。这 3 个认知结构相互迭代并形成推理周期, 动作会形成新的或经过更新的观察, 从而形成新的或经过更新的假设, 然后促使分析师采取后续动作。

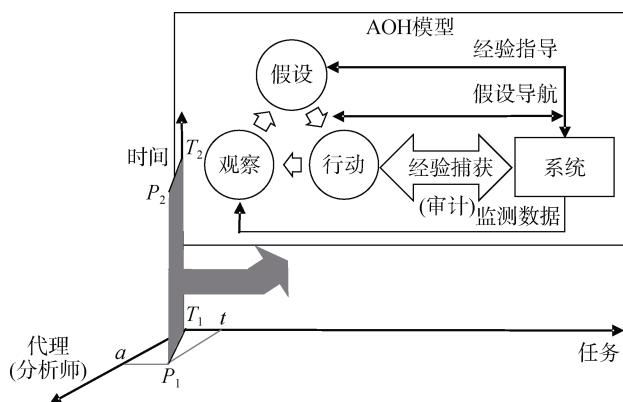


图 7 A-O-H 模型^[9]
Figure 7 A-O-H model^[9]

实际上, 态势理解阶段的认知推理过程就是一个构建 A-O-H 对象的演化过程, 以及对假设进行调查分析和细化完善的演化过程, 我们能基于这些演化过程, 即认知轨迹, 来提取出分析推理的过程。Zhong 等人^[9]研发了采集分析师认知轨迹的工具 ARSCA, 该工具可以为分析师提供两个主要的视图: 数据视图和分析视图。数据视图整合了网络拓扑结构、IDS 告警、防火墙日志等多个监控数据源, 分析视图帮助分析师创建动作、观察和假设的实例, (即 A-O-H 对象)。无经验的分析师可通过学习上述来自经验丰富分析师的认知轨迹, 提升其掌握工控系统态势理解的能力。更重要的是, 这些分析师的认知轨迹可作为案例, 自动分析工控系统中相似的攻击场景。

4.3 评估过程建模技术

工控系统态势理解阶段的三个主要目标是理解攻击者意图、评估系统可靠性和评估任务流程, 下面介绍与三个评估过程相关的模型。

4.3.1 攻击意图模型

我们将工控系统攻击者的意图归纳为破坏业务流程和获取控制权限两种类型。

【破坏业务流程】攻击者可以通过多种方式破坏工控系统的业务流程, 最常见的是数据完整性攻击, 工控系统的数据完整性包括命令完整性和载荷数据完整性, 注入控制流程的可以是开启/关闭控制器、读/写寄存器、上传/下载控制程序等操作命令, 也可以是被篡改的温度、压力等虚假的传感器数据。

大部分破坏业务流程的攻击模式主要是针对电网设计的。Sun 等人^[68]提出了针对智能电网的虚假数据等比例攻击方法, 该方法以相同比例调整连接到被攻击总线的所有相邻传输线的值, 该方法不会改变残差的大小, 因此不会被基于残差的坏数据方案检测出来。Desa 等人^[69]提出了使服务质量下降(service degradation, SD)的工控物理层隐蔽攻击方法, 该方法首先利用 BAS 算法对目标进行系统识别以便获取目标控制系统模型, 然后采用虚假数据注入攻击。Chen 等人^[70]提出了通过篡改自动电压控制器使电网崩溃的攻击模型 POMDP, 该攻击模型利用 Q 强化学习方法帮助攻击者从历史经验中获取最有效的攻击策略。Barreto 等人^[71]提出了针对电网需求响应系统的攻击模型, 该模型不仅能通过突然过载的方式破坏电网设备, 还能通过负载整形的方式欺骗需求响应系统, 这类精心构造的攻击比直接攻击产生的破坏更大。Tan 等人^[72]利用控制理论推导出几何攻击(scaling attacks)和延迟攻击(delay attacks), 并评估这两类攻击对实时电价系统稳定性的影响, 研究表明当攻击者在几何攻击中减小传送给智能电表的价格信号或者在延迟攻击中向一半以上的消费者提供旧电价时, 实时电价系统的稳定性会被破坏。

此外, 还有文献提出通用的工控系统攻击模型, 其中最有影响的是 Li 等人^[73]提出的双环模型。如图 8 所示, 该模型具有攻击环路(attack loop)和掩护环路(covert loop)两条攻击路径, 攻击环路负责将目标系统转移到期望的稳定状态, 掩护环路负责模拟正常的稳定状态以便掩护攻击环路, 这两个过程结合可在不被发现的情况下改变物理系统的稳态。具体来说, 首先基于 LSSVM 技术构建攻击代理以便获取控制器的功能, 并在识别 PID 控制环路的基础上将工控设备的稳定状态移动到期望状态; 其次基于

LSSVM 构建掩护代理, 以便获取工控系统稳定状态的近似模型。

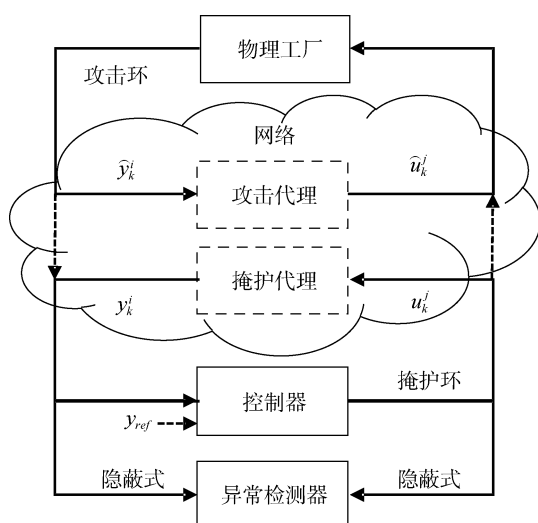


图 8 双环模型^[73]

Figure 8 Two-loop structure^[73]

窃密攻击指工控系统的网络拓扑、设备型号等敏感信息被暴露在互联网上, 攻击者利用这些信息破坏工控系统。Konstantinou 等人^[74]从互联网上获取智能电网的网络结构、控制设备和通信协议等公开信息, 并用实验描述了攻击者如何利用上述公开信息, 通过不同路径修改控制设备的操作等攻击向量。无线通信干扰指攻击者通过射频信号对 IEEE 802.11、IEEE 802.15.4、WirelessHart、ZigBee、Bluetooth 等工控无线通信协议进行干扰, 使其通信过程出现异常。Adepu 等人^[75]利用射频(radio frequency, RF)信号对工控系统的无线链路进行干扰攻击。

【获取控制权限】攻击者主要通过漏洞利用、后门和 rootkit 获取工控系统的控制权限。与传统 IT 系统相比, 获取工控系统权限不仅会破坏系统的完整性、机密性和可用性, 还会直接影响该系统周边员工的人生安全。

Quarta 等人^[76]提出了针对工业机器人的攻击模型, 攻击者利用该模型可获取工业机器人的管理员控制权限, 进而影响该机器人应用的生产过程, 甚至操作机器人伤害附近的员工。Klick 等人^[77]研究了 PLC 的运行环境, 通过在 PLC 的 STL 程序中嵌入 SNMP 扫描和 SOCKS 代理来模拟攻击者植入的后门, 该实验证明攻击者可利用暴露在互联网上的 PLC 渗透进企业生产网和控制网。Garcia 等人^[78]提出了一种名为 HARVEY 的 PLC rootkit, 该 rootkit 驻留在 PLC 固件的控制逻辑以下, 通过拦截、修改传给执行器的控制命令实现隐蔽攻击。Govil 等人^[79]提出了梯

形图逻辑炸弹(ladder logic bombs, LLB)的概念, 并在工控系统测试床验证了功能篡改、系统配置篡改和传输信息篡改三种 LLB 原型。

4.3.2 系统可靠性评估模型

虽然对工控系统攻击者意图理解的相关工作仍在发展, 但一些研究的关注点已经转移到影响评估技术, 希望通过该技术评估恶意攻击对工控系统可靠性的影响。

下面首先讨论系统可靠性量化方法。Huang 等人^[80]利用贝叶斯网络为网络组件、系统漏洞、攻击路径以及攻击成功可能性之间的依赖关系建模。如图 9 所示, 首先, 基于上述贝叶斯模型, 以及态势觉察阶段的入侵检测证据, 可推断出工控系统传感器和执行器被破坏的概率。其次, 以这些概率为输入, 利用随机混杂系统模型(stochastic hybrid system, SHS)预测工控物理过程的演变。最后, 评估网络攻击对工控物理信息系统的风险。 q_0 表示物理系统正常的操作模式, 发生网络攻击时, q_0 会转移到另一种混杂状态。除 q_0 外, 其他混杂状态物理过程的平均关机时间(Mean-Time-To-Shut-Down, MTTSD)被计算, 以便量化瞬时物理信息风险。

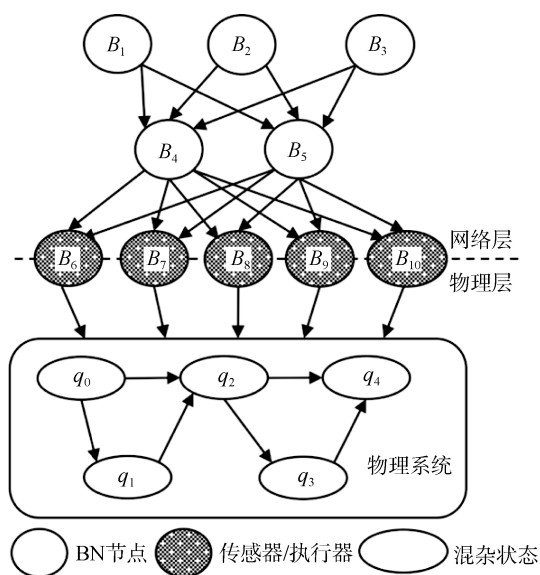


图 9 系统可靠性评估框架^[80]

Figure 9 Proposed risk assessment framework^[80]

4.3.3 任务流程评估模型

实际上, 工控系统风险量化不仅需要考虑攻击对系统可靠性的影响, 还需要考虑攻击对业务流程中工作任务的影响。Holsopple 和 Yang^[81]利用树形结构计算恶意攻击对工作任务的影响, 每棵树表示一个工作任务。基于该树形结构, 分析师能方便地确定哪些资产或工作任务正在受到攻击的影响。图 10 描

述了某特定时间点的工作任务树的基本结构。每棵工作任务树由三种不同类型的节点组成: 资产节点、聚合节点和任务节点。资产节点始终位于叶子节点; 聚合节点表示某种数学函数, 可通过该函数计算所有子节点对其父节点的影响程度; 工作任务节点位于根节点(主工作任务)或者支持主工作任务的一组子工作任务。

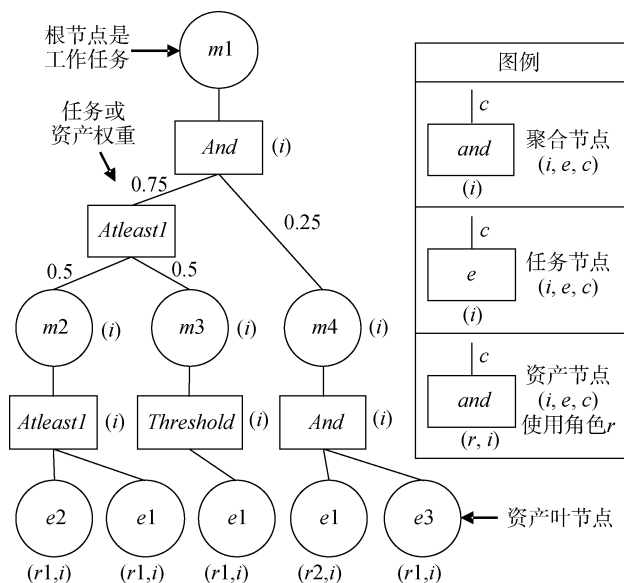


图 10 工作任务树结构^[81]

Figure 10 Mission tree structure^[81]

工作任务树资产节点被定义成一个三元组(i, e, c), e 表示资产标识, c 表示该节点对父工作任务的重

要性, $i \in [0, 1]$ 表示 e 对 c 的影响评分。任务节点也被定义成一个三元组(i, e, c), e 表示工作任务, c 表示该工作任务对父工作任务支持的权重, i 表示工作任务 e 的影响得分。聚合节点也被定义成一个三元组(i, e, c), e 表示聚合函数, 一般选择 Yager 的聚合函数^[82], 关键性是 c , 共同影响是 $i = f(e)$ 。需要注意的是虽然资产节点、任务节点和聚合节点均用三元组表示, 但不同节点的字母含义是不一样的。

Green 等人^[83]利用平均受损时间评估社会工程学对工控系统业务的影响, 并利用量化的风险受损图识别易受社会工程学影响的节点。Abdo 等人^[84]利用 Bow-Tie 结构为工控系统事故建模, 分析师可利用该模型向前分析导致事故发生的原因, 向后分析该事件的后续事件, 以便针对性地设置屏障进行防控。Motzek 等人^[85]为每个专家的经验构建概率统计模型, 并将上述不同专家知识整合成统一的工作任务影响评估模型。

5 工控系统安全态势投射

工控系统安全态势投射阶段的基本任务是展望当前态势将如何演化至未来态势, 以及对未来态势中元素的预期, 回答“那将会怎样”的问题。如图 11 所示, 工控系统安全态势投射阶段, 攻击图、贝叶斯网络、马尔科夫模型被用来构建攻击模型, 预测可能的攻击事件, 预测可能被病毒感染的目标资产, 预测可能的零日漏洞。

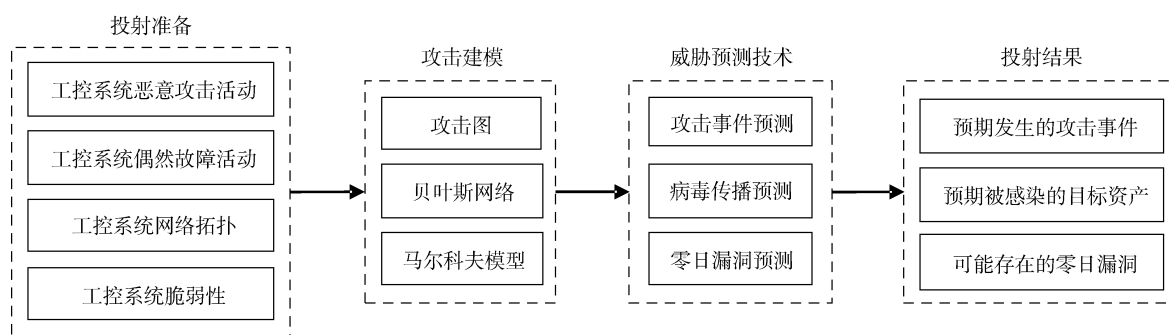


图 11 工控系统安全态势投射模型

Figure 11 Projection model of situational awareness for industrial control systems security

5.1 攻击模型构建

攻击预测主要利用攻击图、贝叶斯网络和马尔科夫模型进行建模, 本小结主要讨论这 3 种技术。

5.1.1 攻击图

攻击图是一种利用树形结构表示攻击场景的方法, 攻击图是贝叶斯网络和马尔科夫模型的基础。攻击图可以表示成 $G = (S, r, S_0, S_s)$, 其中 S 表示状态集合, $r \subseteq S * S$, 表示状态转移关系, $S_0 \subseteq S$ 表示初始

状态集合, $S_s \subseteq S$ 表示成功状态集合。初始状态表示攻击开始之前的状态, 转移关系表示攻击者可能的动作。若攻击者从初始状态到达任何一个成功状态, 则说明攻击是成功的, 成功状态表示攻击者达到的目标。攻击图既可自动化构建, 也可通过手工方式构建, 最流行的是利用数据挖掘技术生成攻击图^[86]。如图 12 所示, 节点表示可能的攻击事件, 如“ICMP PING”表示攻击者发起扫描动作; 边的权重表示箭

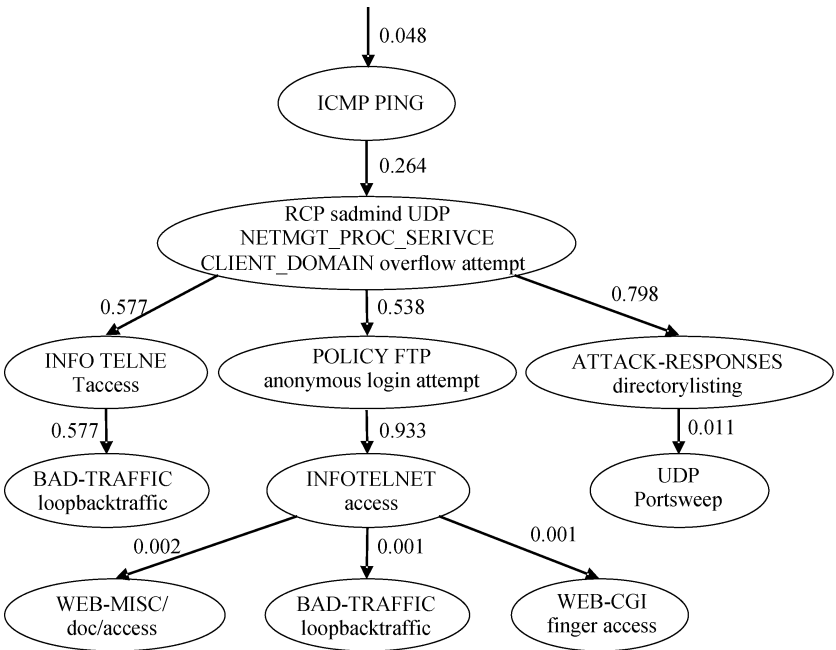


图 12 基于漏洞利用的攻击图示例^[86]

Figure 12 Example of exploit-oriented attack graph^[86]

头结束的节点发生攻击事件的概率，如 0.048 表示攻击者以 4.8% 的概率发起 Ping 扫描动作。这些概率是通过历史数据统计出来的。

Xia 等人^[87]构建了辅助分析师的工控系统攻击路径建模和分析系统，该系统具有网络建模、推理规则建模、攻击树建模和安全分析等功能，还能利用多目标优化方法生成一组防御策略。Sabaliauskaite 等人^[48]利用“目标树-成功树”(Goal Tree Success Tree, GTST)为工控系统建模，并利用 GTST 分析工控系统的功能安全。Wang 等人^[88]基于攻击图和最大流量为

网络节点的攻击行为建模，并利用通用漏洞评分系统量化节点受到的攻击风险。

5.1.2 贝叶斯网络

一种攻击图的替代方法是贝叶斯网络。通过将告警映射至攻击类别并进行概率推导，动态贝叶斯网络可根据经验(训练数据)预测未来所有可能的动作。贝叶斯网络是概率图模型，该模型表示变量以及变量之间的关系，每个节点保存着随机变量及其条件概率。每个节点表示一个变量，每个变量包含多个状态，边表示节点间的因果关系。如图 13 所示，贝

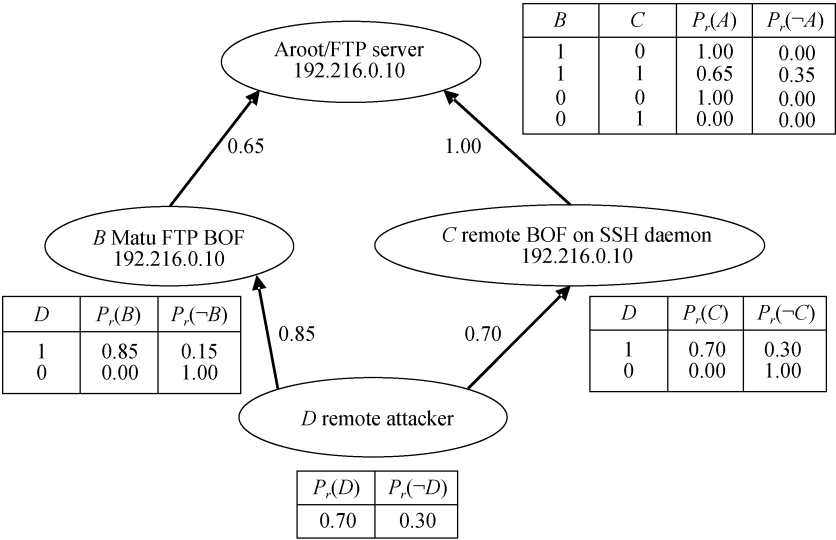


图 13 贝叶斯攻击图概率计算示例^[89]

Figure 13 Example of bayesian attack graph for probability computations^[89]

叶斯网络为攻击者 D 建模, 该攻击者试图利用缓冲区漏洞 B 或 C 获取服务器 A 的访问权限^[89]。首先, 给攻击者 D 赋予概率 $Pr(D) = 0.7$, 这个概率表示专家对目标系统可能遭受远程攻击的主观置信度。边上的权重表示漏洞利用成功的概率, 如: 边“ $D \rightarrow B$ ”上的权重 0.85 表示攻击者 D 利用 B 上漏洞成功的概率。节点概率表描述了攻击者可能利用该节点的父节点们漏洞的成功概率, 如: A 节点概率表中“ $B=1, C=0$ ”表示攻击者利用 B 节点漏洞, 不利用 C 节点漏洞成功访问 A 的概率是 0.65。

Huang 等人^[90]采集攻击者和防御者多个阶段的不完整信息, 并分别为攻击者和防御者构建动态贝叶斯网络, 当攻防双方达到贝叶斯纳什均衡状态时, 任何一方都不能通过单独行动改变现状, 该状态可用于预测攻防双方的下一步操作。Zhang 等人^[91]通过多级贝叶斯网络整合攻击知识、系统功能和危险事件, 同时降低事件预测的复杂性; 然后利用上述攻击知识和系统知识分析攻击的潜在影响; 最后通过统一的风险量化方法计算多个工控事件的安全风险。Huang 等人^[80]利用贝叶斯网络为攻击传播过程建模, 并通过该攻击传播模型预测传感器和执行器被破坏的概率。

5.1.3 马尔科夫模型

另一种常见的攻击预测方法是马尔科夫模型(Markov Models)马尔科夫模型包括马尔科夫链和隐马尔科夫模型(Hidden Markov Model, HMM)。马尔科夫模型常采用图的形式表示, 这与攻击图和贝叶斯网络比较相似。态势觉察阶段会产生告警序列, 为从

这些告警序列构建 HMM, 需要确定模型的状态数量、每个状态可观测变量的种类、状态转移概率分布和初始状态分布。状态数量即攻击类型的数量, 可观测变量即告警, 状态转移和可观测变量转移概率均来自历史记录。相比攻击图和贝叶斯网络, 马尔科夫模型的优势是, 即使出现漏报(未检测到某些攻击步骤), 该模型依然可以很好地工作。

Li 等人^[92]利用马尔科夫随机过程技术为控制系统建模, 基于频域变换技术和线性代数理论推理出随机网络攻击和干扰发生的充分必要条件。Caselli 等人^[93]基于离散时间和马尔科夫链为工控设备的操作建模, 并利用该模型从过程变量中检测顺序篡改和时序篡改两类序列攻击事件。

5.2 威胁预测

攻击事件、病毒和零日漏洞是工控系统面临的三个主要威胁。下面讨论如何利用最先进的技术, 基于态势觉察到的可疑活动以及态势理解构建的业务本体模型, 预测上述三种威胁。

5.2.1 攻击事件预测

网络攻击是工控系统面临的主要威胁。2016 年, “沙虫”组织对乌克兰电力 SCADA 系统发起网络攻击, 导致数个街区发生大规模停电事件^[3]。2019 年, 委内瑞拉发生了大规模停电事件, 该事件已经被充分论证为网络攻击^[4]。电力等工控系统是关乎社会稳定的国家关键基础设施, 需提早预测对其的网络攻击, 为应急响应争取时间。Zhang 等人^[91]利用多级贝叶斯网络预测工控系统危险事故, 并利用模拟的石化仿真平台验证预测方法的准确性。如图 14 所示,

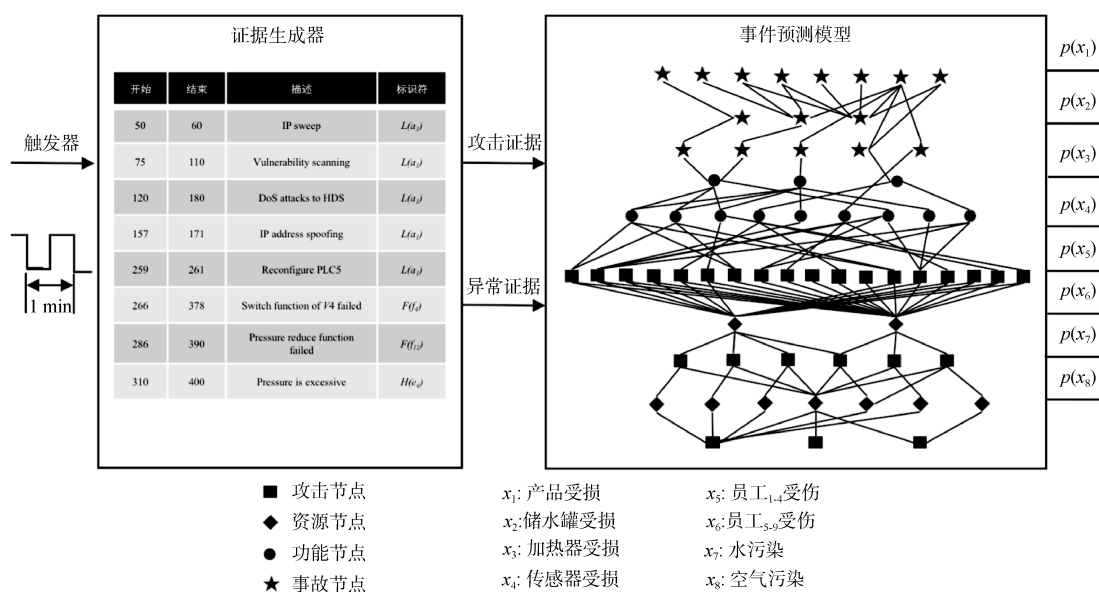


图 14 基于多级贝叶斯网络的攻击事件预测平台架构^[91]

Figure 14 Structure of the attack event simulation platform based on multilevel bayesian networks^[91]

模拟平台是利用 MATLAB 实现的, 该平台由证据生成器、事故预测和风险评估三个模块构成, 本章节主要讨论事件预测模块。

证据来自态势觉察阶段生成的告警、控制操作等攻击事件线索, 通过一个数组存储上述证据列表。多级贝叶斯网络的每个节点都有一个唯一索引, 索引范围是 $1 \sim N$, N 表示节点总数量, 数组元素的取值范围是 $-N \sim N$ 的整数。若数组中第 i 个元素是 0, 表示第 i 分钟无证据; 若数组中第 i 个元素是整数, 表示第 i 分钟有整数个证据; 若数组中第 i 个元素是负数, 表示证据在第 i 分钟被撤回。证据生成器的输入是一个时间触发器(trigger), 当证据生成器收到一个触发时, 它会读取输入时间, 并根据数组更新多级贝叶斯网络的证据集合。事故预测模块使用 MATLAB 的贝叶斯网络工具集建立多级贝叶斯网络。当证据生成器发送证据时, 这些证据将被添加到证据集合 E 中。随后基于证据集合 E , 事故预测模块使用贝叶斯网络工具集推理贝叶斯网络。最后, 计算出 x_1, x_2, \dots, x_8 等事件发生的概率。

5.2.2 病毒传播预测

工控系统面临的另一种主要威胁是病毒。Stuxnet 病毒重创了布什尔核电站的离心机, 导致伊朗推迟其核计划^[1]。Zimba 等人^[94]详细分析了 WannaCry 蠕虫, 并对其多个攻击节点进行建模。Antonakakis 等人^[95]分析了设备被 Mirai 蠕虫感染的过程, 并对其变体的演化历史进行了总结。Lee 等人^[3]分析了 BlackEnergy 病毒的工作原理, 并分析了其破坏乌克兰电网的过程。实际上, 工控系统非常容易受到传统 IT 系统病毒的攻击, Windows 系统存在的漏洞已经给工控系统带来了巨大损失^[96]。

为从 PC 网络向控制网络传输程序或调整的工艺参数, 或者从控制网络收集历史业务数据, 需将 PC 网络与控制网络连接起来。这样的拓扑结构使病毒在 PC 网络和控制网络之间的传播成为可能。Yao 等人^[10]研究了 PLC-PC 蠕虫的传播模型和防御模型, 发现该类蠕虫在 PC 网络存在易感染(susceptible)、已感染(infectious)、隔离(quarantined)和恢复(recovered) 4 种状态, 在 PLC 网络存在的易感染、已感染和恢复三种状态。Yao 等人进一步指出了病毒在 PLC 网络不存在隔离状态的两个原因, 分别是(1)PLC 没有 PC 那样强大的处理器, 无法运行隔离补丁; (2)PLC 执行的是实时任务, 强制隔离会导致生产过程中断。基于上述发现, Yao 等人分析了病毒在 PC 网络和 PLC 网络的状态转移情况。如图 15 所示, $N_{i,j}^A$ 表示度为 (i, j) 的 PC 节点数量, (i, j) 节点表示该节点与 PC 网络内的

i 个节点连接, 与 PLC 网络内的 j 个节点连接。 $\mu_1 N_{i,j}^A$ 表示新节点以概率 μ_1 被加入 PC 网络, 这些 $b\mu_1 N_{i,j}^A$ 节点进入已感染状态的概率是 b 。 S^A 表示 PC 网络中的资产正处于易感染状态, 该资产从已感染状态 S^A 转移到易感染状态 I^A 的概率是 $\beta_{11} i S_{i,j}^A \Theta_{11}(t)$ 。

进一步, Yao 等人计算出病毒在 PC 网络和 PLC 网络达到平衡状态所需的条件。理想情况是 PC-PLC 网络无病毒, 这种情况不仅要求 PC 网络和 PLC 网络均不存在已感染的节点, 还要求无状态发生变化, 即所有状态的转移概率为 0。理想情况通常难以实现, 作者求解了 PC-PLC 网络存在部分已感染节点, 但不再有新的节点被感染这种情况所需的平衡条件。求解上述两种平衡状态, 即可预测病毒在 PC-PLC 网络中的传播趋势。

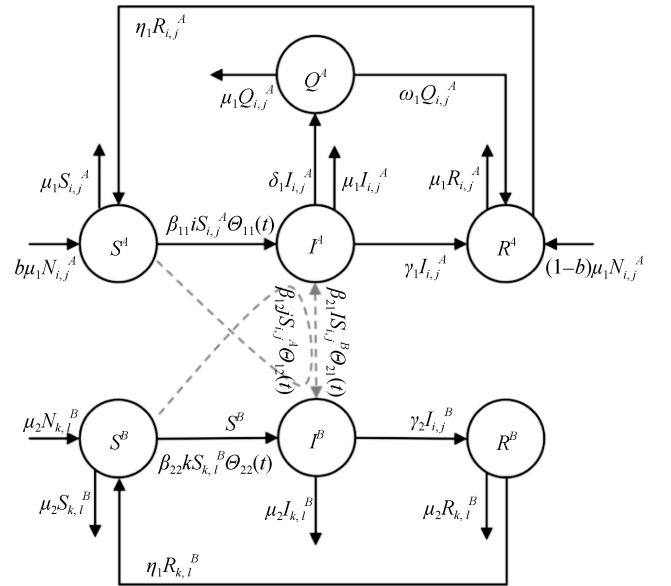


图 15 PLC-PC 网络中节点状态之间的转换^[10]
Figure 15 The transition diagram among the states of the nodes in PLC-PC network^[10]

5.2.3 零日漏洞预测

零日漏洞也是工控系统面临的主要威胁。这些漏洞常常被攻击者利用, 以躲避可疑活动识别工具的检测。McLaughlin 等人^[97]总结了工控系统硬件层、固件层、软件层、网络层和控制过程层的漏洞特点及其被攻击者利用的动机。2015 年, 两名黑客利用汽车的无线控制软件的零日漏洞, 展示了如何远程操纵汽车的仪表盘、转向、制动和传动装置^[98]。Zimba 等人^[94]发现 WannaCry 等工控病毒通常在发现 SCADA 系统和控制设备存在的漏洞后, 才开始在控制网络中传播。因此, 对零日漏洞的预测具有重要的

现实意义。实际上,攻击者为了达到目标仅利用零日漏洞是不可能的,他们通常会利用一些已知漏洞,可通过这些已知漏洞触发的告警调查零日漏洞。

Dai 等人^[9]提出了零日攻击路径发现工具 Patrol。该工具的工作过程如下:首先,根据过滤规则从系统调用日志提取出单个设备的访问路径;随后,基于上述访问路径为每台设备构建进程、文件和 sockets 对象依赖图,并根据网络拓扑将这些设备级对象依赖图扩展为网络级对象依赖图;然后,采用广度优先算法以触发点(IDS 等的告警)为种子节点向后沿着反向边找到入侵的开始节点,并采用广度优先算法以触发点为种子节点向前沿着有向边找到受影响的后续节点;最后,通过影子指标(Shadow indicator)识别候选零日攻击路径,这些路径由被感染概率最大的节点及其中间节点构成。候选的零日攻击路径包含了未知的漏洞,可通过人工方式验证这些零日漏洞。

6 工控系统安全态势感知待解决问题

尽管学术界和工业界在工控系统安全态势感知领域取得了较大进步,但仍存在 5 个待解决的问题,下面分别介绍每个问题的研究思路。

6.1 态势觉察阶段

6.1.1 扫描技术对工控系统稳定性的影响

当前的网络拓扑测绘和脆弱性发现技术主要采用扫描地方式获取工控系统的网络拓扑和脆弱性信息,这些扫描行为会显著增加工控网络的时延,降低工控系统的运行效率,甚至破坏工控业务流程。可通过纯被动方式从网络流中获取工控系统的资产、服务、任务及其相互关系,但纯被动方式无法解析私有协议中的复杂字段。因此,需研究低干扰工控网络探测技术,在复杂多变的工控网络拓扑结构中实时更新网络拓扑和脆弱性信息。

6.1.2 觉察工具可靠性验证

入侵检测、入侵诱捕、防火墙等态势感知觉察工具容易遭受欺骗或攻击,导致这些数据不被信任。分析师高度依赖上诉觉察源数据,为验证这些数据源是否遭到攻击,需不断地手动检测觉察源的置信度。因此,需要设计实时的觉察源可靠性自动分析工具,不断测试觉察源数据是否满足所需的置信度,且这些方法不能显著影响工控系统的正常工作。

6.2 态势理解阶段

6.2.1 工控实体行为动态建模

为了在态势理解阶段实现自动化推理能力,需要抽取操作员站、PLC、HMI 等工控实体的安全属

性,如漏洞等信息,并描述工控系统的计算过程和物理过程,构建工控系统安全本体模型。目前还没有这方面的工作,一个可行的方案是基于军事领域的本体模型 UCORE-SL,利用 OWL 格式对工控系统对象和业务流程进行建模。

6.2.2 混淆技术对攻击建模的影响

工控系统涉及用户、防御者和攻击者三类对象,分析师觉察到的绝大部分活动是用户的合法活动,但用户经常会因为缺乏经验和错误操作产生大量可疑活动,分析师很难将这些误操作与恶意攻击区分开。另外,攻击者尝尝采用噪声注入、轨迹擦除、告警篡改等技巧混淆攻击序列。因此,分析师不仅需要充分理解工控系统环境,还需要很好地理解普通用户的行为,以及相关任务、目标和误操作,并在此基础上掌握攻击者的意图、能力、目标和习惯。

6.3 态势投射阶段

针对工控系统的 APT 攻击在启动攻击前会开展前期探测和验证工作,如检测控制器型号是否匹配,可基于这些前期活动预测随后的破坏性攻击。但這些前期活动在时间轴上的分布较为分散,且常伪装为正常的用户活动。为防止计算资源被耗尽,传统的关联技术仅能分析一段时间内的可疑活动,因此难以发现上述攻击活动之间的联系,更难以推测攻击者下一步的计划。一个可行的方案是采用杀伤链技术,将已经发现的攻击活动映射到杀伤链上,判断该 APT 攻击当前所处的阶段,大致推测攻击者下一步的目标,并将计算资源转移到该目标上,保持对 APT 攻击的持续跟踪。

7 总结

本文利用现有的工控安全技术构建了工控系统安全态势感知模型,该模型包括态势觉察、态势理解和态势投射三个阶段。态势觉察阶段利用入侵检测等多种安全工具发现可疑活动,并借助扫描技术提取上述活动的网络拓扑和脆弱性等上下文信息。态势理解阶段首先基于本体模型为工控任务间的依赖关系和工控任务与资产映射关系建模,随后利用粗粒度和细粒度两种认知推理方法理解攻击者意图,并评估工控业务受到可疑活动的影响。态势投射阶段利用攻击图等模型预测工控系统可能发生的攻击事件、可能被病毒感染的资产以及可能存在的零日漏洞。本篇论文是总结工控系统安全态势感知研究进展的综述性文章。

近些年,工控系统安全态势感知技术取得了大量研究成果,但距离实际应用还存在不小差距。

网络扫描等技术会对工控系统的稳定性造成较大影响, 需研究低干扰的工控网络探测技术。入侵检测等态势觉察工具容易被攻击或欺骗, 需要不断验证这些工具的可靠性。误操作、告警篡改等因素导致工控系统中隐藏的攻击活动很难被区分出来, 需研究更准确的用户行为和攻击者行为理解技术。尚没有通用的工控系统安全本体模型, 可借助军事领域的本体模型和 OWL 格式对工控系统实体行为进行动态建模。传统的攻击关联技术难以预测针对工控系统 APT 攻击的下一步计划, 可采用杀伤链技术推测攻击者的下一步目标, 并保持对 APT 攻击的持续跟踪。

参考文献

- [1] Weinberger S. Computer Security: Is this the Start of Cyberwarfare? [J]. *Nature*, 2011, 474(7350): 142-145.
- [2] R. Lee, M. Assante, T. Connway. German steel mill cyber attack. Technical report. Sans ICS, 2014.
- [3] R. M. Lee, M. J. Assante, T. Conway. Analysis of the cyber attack on the Ukrainian power grid. Technical report. E-ISAC, 2016.
- [4] Ricardo V. Venezuela's Power Grid Disabled by Cyber Attack[J]. *Green Left Weekly*, 2019(1213): 15-29.
- [5] Urbina D I, Giraldo J A, Cardenas A A, et al. Limiting the Impact of Stealthy Attacks on Industrial Control Systems[C]. *The 2016 ACM SIGSAC Conference on Computer and Communications Security*, 2016: 1092-1105.
- [6] Abbasi A, Holz T, Zambon E, et al. ECFI: Asynchronous Control Flow Integrity for Programmable Logic Controllers[C]. *The 33rd Annual Computer Security Applications Conference*, 2017: 437-448.
- [7] Vasilomanolakis E, Srinivasa S, Cordero C G, et al. Multi-Stage Attack Detection and Signature Generation with ICS Honey-pots[C]. *NOMS 2016 - 2016 IEEE/IFIP Network Operations and Management Symposium*, 2016: 1227-1232.
- [8] Kriaa S, Pietre-Cambacedes L, Bouissou M, et al. A Survey of Approaches Combining Safety and Security for Industrial Control Systems[J]. *Reliability Engineering & System Safety*, 2015, 139: 156-178.
- [9] Zhong C, Kirubakaran D S, Yen J, et al. How to Use Experience in Cyber Analysis: An Analytical Reasoning Support System[C]. *2013 IEEE International Conference on Intelligence and Security Informatics*, 2013: 263-265.
- [10] Yao Y, Sheng C, Fu Q, et al. A Propagation Model with Defensive Measures for PLC-PC Worms in Industrial Networks[J]. *Applied Mathematical Modelling*, 2019, 69: 696-713.
- [11] Teixeira A, Sou K C, Sandberg H, et al. Secure Control Systems: A Quantitative Risk Management Approach[J]. *IEEE Control Systems Magazine*, 2015, 35(1): 24-45.
- [12] Endsley M R. Toward a Theory of Situation Awareness in Dynamic Systems[J]. *Human Factors: the Journal of the Human Factors and Ergonomics Society*, 1995, 37(1): 32-64.
- [13] Galloway B, Hancke G P. Introduction to Industrial Control Networks[J]. *IEEE Communications Surveys & Tutorials*, 2013, 15(2): 860-880.
- [14] Wressnegger C, Kellner A, Rieck K. ZOE: Content-Based Anomaly Detection for Industrial Control Systems[C]. *2018 48th Annual IEEE/IFIP International Conference on Dependable Systems and Networks*, 2018: 127-138.
- [15] Adhikari U, Morris T H, Pan S Y. Applying Hoeffding Adaptive Trees for Real-Time Cyber-Power Event and Intrusion Classification[J]. *IEEE Transactions on Smart Grid*, 2018, 9(5): 4049-4060.
- [16] Feng C, Li T T, Chana D. Multi-Level Anomaly Detection in Industrial Control Systems via Package Signatures and LSTM Networks[C]. *2017 47th Annual IEEE/IFIP International Conference on Dependable Systems and Networks*, 2017: 261-272.
- [17] Ponomarev S, Atkison T. Industrial Control System Network Intrusion Detection by Telemetry Analysis[J]. *IEEE Transactions on Dependable and Secure Computing*, 2016, 13(2): 252-260.
- [18] Yun J H, Hwang Y, Lee W, et al. Statistical Similarity of Critical Infrastructure Network Traffic Based on Nearest Neighbor Distances[C]. *Research in Attacks, Intrusions, and Defenses*, 2018: 577-599.
- [19] Dunlap S, Butts J, Lopez J, et al. Using Timing-Based Side Channels for Anomaly Detection in Industrial Control Systems[J]. *International Journal of Critical Infrastructure Protection*, 2016, 15: 12-26.
- [20] Haller P, Genge B, Duka A V. On the Practical Integration of Anomaly Detection Techniques in Industrial Control Applications[J]. *International Journal of Critical Infrastructure Protection*, 2019, 24: 48-68.
- [21] Haller P, Genge B, Duka A V. Engineering Edge Security in Industrial Control Systems *Critical Infrastructure Security and Resilience*, 2019: 185-200.
- [22] Qadeer R, Murguia C, Ahmed C M, et al. Multistage Downstream Attack Detection in a Cyber Physical System[C]. *Computer Security*, 2018: 177-185.
- [23] Krotofil M, Larsen J, Gollmann D. The Process Matters: Ensuring Data Veracity in Cyber-Physical Systems[C]. *The 10th ACM Symposium on Information, Computer and Communications Security*, 2015: 133-144.
- [24] Pal K, Adepu S, Goh J. Effectiveness of Association Rules Mining for Invariants Generation in Cyber-Physical Systems[C]. *2017 IEEE 18th International Symposium on High Assurance Systems Engineering*, 2017: 124-127.
- [25] Cheng L, Tian K, Yao D D. Orpheus: Enforcing Cyber-Physical Execution Semantics to Defend Against Data-Oriented Attacks[C]. *The 33rd Annual Computer Security Applications Conference*, 2017: 315-326.
- [26] Hu Y, Li H, Luan T H, et al. Detecting Stealthy Attacks on Industrial Control Systems Using a Permutation Entropy-Based Method[J]. *Future Generation Computer Systems*, 2020, 108: 1230-1240.
- [27] Aoudi W, Iturbe M, Almgren M. Truth will Out: Departure-Based Process-Level Detection of Stealthy Attacks on Control Systems[C]. *The 2018 ACM SIGSAC Conference on Computer and*

- Communications Security*, 2018: 817-831.
- [28] SICARD F, ZAMAI É, FLAUS J M. An Approach Based on Behavioral Models and Critical States Distance Notion for Improving Cybersecurity of Industrial Control Systems[J]. *Reliability Engineering & System Safety*, 2019, 188: 584-603.
 - [29] Khalili A, Sami A. SysDetect: A Systematic Approach to Critical State Determination for Industrial Intrusion Detection Systems Using Apriori Algorithm[J]. *Journal of Process Control*, 2015, 32: 154-160.
 - [30] Han Y, Etigowni S, Liu H, et al. Watch Me, but Don't Touch Me! Contactless Control Flow Monitoring via Electromagnetic Emanations[C]. *The 2017 ACM SIGSAC Conference on Computer and Communications Security*, 2017: 1095-1108.
 - [31] Yang A, Wang X S, Sun Y Y, et al. Multi-Dimensional Data Fusion Intrusion Detection for Stealthy Attacks on Industrial Control Systems[C]. *2018 IEEE Global Communications Conference*, 2018: 1-7.
 - [32] Ahmed C M, Ochoa M, Zhou J Y, et al. NoisePrint: Attack Detection Using Sensor and Process Noise Fingerprint in Cyber Physical Systems[C]. *The 2018 on Asia Conference on Computer and Communications Security*, 2018: 483-497.
 - [33] Khalili A, Sami A, Khozaei A, et al. SIDS: State-Based Intrusion Detection for Stage-Based Cyber Physical Systems[J]. *International Journal of Critical Infrastructure Protection*, 2018, 22: 113-124.
 - [34] Vollmer T, Manic M. Cyber-Physical System Security with Deceptive Virtual Hosts for Industrial Control Networks[J]. *IEEE Transactions on Industrial Informatics*, 2014, 10(2): 1337-1347.
 - [35] Winn M, Rice M, Dunlap S, et al. Constructing Cost-Effective and Targetable Industrial Control System Honeypots for Production Networks[J]. *International Journal of Critical Infrastructure Protection*, 2015, 10: 47-58.
 - [36] Buza D I, Juhász F, Miru G, et al. CryPLH: Protecting Smart Energy Systems from Targeted Attacks with a PLC Honeypot[C]. *Smart Grid Security*, 2014: 181-192.
 - [37] L. Rist, J. Vestergaard, D. Haslinger, et al. CONPOT ICS/SCADA honeypot. Conpot. <http://conpot.org>. June. 2019.
 - [38] Irvine C, Formby D, Litchfield S, et al. HoneyBot: A Honeypot for Robotic Systems[J]. *Proceedings of the IEEE*, 2018, 106(1): 61-70.
 - [39] Rrushi J L. Multi-range Decoy I/O Defense of Electrical Substations Against Industrial Control System Malware *Resilience of Cyber-Physical Systems*, 2019: 151-175.
 - [40] Fang H J, Ye H, Zhong M Y. Fault Diagnosis of Networked Control Systems[J]. *Annual Reviews in Control*, 2007, 31(1): 55-68.
 - [41] Gu Z H, Wang C, Zhang M, et al. WCET-Aware Partial Control-Flow Checking for Resource-Constrained Real-Time Embedded Systems[J]. *IEEE Transactions on Industrial Electronics*, 2014, 61(10): 5652-5661.
 - [42] Rajabpour N, Sedaghat Y. A Software-Based Error Detection Technique for Monitoring the Program Execution of RTUs in SCADA[C]. *Computer Safety, Reliability, and Security*, 2015: 457-470.
 - [43] Canto dos Santos J V, Costa I F, Nogueira T. New Genetic Algorithms for Contingencies Selection in the Static Security Analysis of Electric Power Systems[J]. *Expert Systems With Applications*, 2015, 42(6): 2849-2856.
 - [44] Weimer J, Ivanov R, Chen S J, et al. Parameter-Invariant Monitor Design for Cyber-Physical Systems[J]. *Proceedings of the IEEE*, 2018, 106(1): 71-92.
 - [45] Pan S Y, Morris T, Adhikari U. Developing a Hybrid Intrusion Detection System Using Data Mining for Power Systems[J]. *IEEE Transactions on Smart Grid*, 2015, 6(6): 3104-3113.
 - [46] Wolf M, Serpanos D. Safety and Security in Cyber-Physical Systems and Internet-of-Things Systems[J]. *The IEEE*, 2018, 106(1): 9-20.
 - [47] Zhou M, Lv S C, Yin L B, et al. SCTM: A Multi-View Detecting Approach Against Industrial Control Systems Attacks[C]. *ICC 2019-2019 IEEE International Conference on Communications*, 2019: 1-6.
 - [48] Sabaliauskaite G, Adepu S, Mathur A. A Six-Step Model for Safety and Security Analysis of Cyber-Physical Systems[C]. *Critical Information Infrastructures Security*, 2017: 189-200.
 - [49] Castellanos J H, Ochoa M, Zhou J Y. Finding Dependencies between Cyber-Physical Domains for Security Testing of Industrial Control Systems[C]. *The 34th Annual Computer Security Applications Conference*, 2018: 582-594.
 - [50] Adepu S, Mathur A, Gunda J, et al. An Agent-Based Framework for Simulating and Analysing Attacks on Cyber Physical Systems[C]. *Algorithms and Architectures for Parallel Processing*, 2015: 785-798.
 - [51] Nai Fovino I, Coletta A, Carcano A, et al. Critical State-Based Filtering System for Securing SCADA Network Protocols[J]. *IEEE Transactions on Industrial Electronics*, 2012, 59(10): 3943-3950.
 - [52] Li D, Guo H Q, Zhou J Y, et al. SCADAWall: A CPI-Enabled Firewall Model for SCADA Security[J]. *Computers & Security*, 2019, 80: 134-154.
 - [53] Caselli M, Hadžiosmanović D, Zambon E, et al. On the Feasibility of Device Fingerprinting in Industrial Control Systems[C]. *Critical Information Infrastructures Security*, 2013: 155-166.
 - [54] Feng X, Li Q, Wang H N, et al. Characterizing Industrial Control System Devices on the Internet[C]. *2016 IEEE 24th International Conference on Network Protocols*, 2016: 1-10.
 - [55] Formby D, Srinivasan P, Leonard A, et al. Who's in Control of your Control System? Device Fingerprinting for Cyber-Physical Systems[C]. *Proceedings 2016 Network and Distributed System Security Symposium*, 2016: 21-24.
 - [56] Mirian A, Ma Z E, Adrian D, et al. An Internet-Wide View of ICS Devices[C]. *2016 14th Annual Conference on Privacy, Security and Trust*, 2016: 96-103.
 - [57] Jakobson G. Mission Cyber Security Situation Assessment Using Impact Dependency Graphs[C]. *14th International Conference on Information Fusion*, 2011: 1-8.
 - [58] Rouf I, Mustafa H, Xu M, et al. Neighborhood Watch: Security and Privacy Analysis of Automatic Meter Reading Systems[C]. *The 2012 ACM conference on Computer and communications security*, 2012: 462-473.
 - [59] Shirani P, Collard L, Agba B L, et al. BINARM: Scalable and Efficient Detection of Vulnerabilities in Firmware Images of Intelli-

- gent Electronic Devices[C]. *Detection of Intrusions and Malware, and Vulnerability Assessment*, 2018: 114-138.
- [60] Zhu R J, Zhang B F, Mao J J, et al. A Methodology for Determining the Image Base of ARM-Based Industrial Control System Firmware[J]. *International Journal of Critical Infrastructure Protection*, 2017, 16: 26-35.
- [61] Gruber T. Ontology[M]. *Encyclopedia of Database Systems*. Boston, MA: Springer US, 2009: 1963-1965.
- [62] Ulicny B E, Moskal J J, Kokar M M, et al. Inference and Ontologies[Cyber Defense and Situational Awareness], 2014: 167-199.
- [63] Holsopple J, Yang S J. FuSIA: Future Situation and Impact Awareness[C]. *2008 11th International Conference on Information Fusion*, 2008: 1-8.
- [64] Rocchetto M, Tippenhauer N O. Towards Formal Security Analysis of Industrial Control Systems[C]. *The 2017 ACM on Asia Conference on Computer and Communications Security*, 2017: 114-126.
- [65] Cheminod M, Durante L, Seno L, et al. Semiautomated Verification of Access Control Implementation in Industrial Networked Systems[J]. *IEEE Transactions on Industrial Informatics*, 2015, 11(6): 1388-1399.
- [66] J. Yen, RF. Erbacher, C. Zhong, et al. Cognitive Process[C]. *Cyber Defense and Situational Awareness*, 2014: 119-144.
- [67] Coppolino L, D'Antonio S, Formicola V, et al. Enhancing SIEM Technology to Protect Critical Infrastructures[C]. *Critical Information Infrastructures Security*, 2013: 10-21.
- [68] Sun Y, Li W T, Song W T, et al. False Data Injection Attacks with Local Topology Information Against Linear State Estimation[C]. *2015 IEEE Innovative Smart Grid Technologies - Asia*, 2015: 1-5.
- [69] de Sá A O, da Costa Carmo L F R, Machado R C S. Covert Attacks in Cyber-Physical Control Systems[J]. *IEEE Transactions on Industrial Informatics*, 2017, 13(4): 1641-1651.
- [70] Chen Y, Huang S W, Liu F, et al. Evaluation of Reinforcement Learning-Based False Data Injection Attack to Automatic Voltage Control[J]. *IEEE Transactions on Smart Grid*, 2019, 10(2): 2158-2169.
- [71] Barreto C, Cárdenas A A, Quijano N, et al. CPS: Market Analysis of Attacks Against Demand Response in the Smart Grid[C]. *The 30th Annual Computer Security Applications Conference*, 2014: 136-145.
- [72] Tan R, Krishna V B, Yau D K Y, et al. Impact of Integrity Attacks on Real-Time Pricing in Smart Grids[C]. *The 2013 ACM SIGSAC conference on Computer & communications security*, 2013: 439-450.
- [73] Li W Z, Xie L, Wang Z L. Two-Loop Covert Attacks Against Constant Value Control of Industrial Control Systems[J]. *IEEE Transactions on Industrial Informatics*, 2019, 15(2): 663-676.
- [74] Konstantinou C, Sazos M, Maniatakos M. Attacking the Smart Grid Using Public Information[C]. *2016 17th Latin-American Test Symposium*, 2016: 105-110.
- [75] Adepu S, Prakash J, Mathur A. WaterJam: An Experimental Case Study of Jamming Attacks on a Water Treatment System[C]. *2017 IEEE International Conference on Software Quality, Reliability and Security Companion*, 2017: 341-347.
- [76] Quarta D, Pogliani M, Polino M, et al. An Experimental Security Analysis of an Industrial Robot Controller[C]. *2017 IEEE Symposium on Security and Privacy*, 2017: 268-286.
- [77] Klick J, Lau S, Marzin D, et al. Internet-Facing PLCs as a Network Backdoor[C]. *2015 IEEE Conference on Communications and Network Security*, 2015: 524-532.
- [78] Garcia L A, Brasser F, Cintuglu M H, et al. Hey, my Malware Knows Physics! Attacking PLCs with Physical Model Aware Rootkit[C]. *2017 Network and Distributed System Security Symposium*, 2017: 1-15.
- [79] Govil N, Agrawal A, Tippenhauer N O. On Ladder Logic Bombs in Industrial Control Systems[C]. *Computer Security*, 2018: 110-126.
- [80] Huang K X, Zhou C J, Tian Y C, et al. Assessing the Physical Impact of Cyberattacks on Industrial Cyber-Physical Systems[J]. *IEEE Transactions on Industrial Electronics*, 2018, 65(10): 8153-8162.
- [81] Holsopple J, Yang S J. Handling Temporal and Functional Changes for Mission Impact Assessment[C]. *2013 IEEE International Multi-Disciplinary Conference on Cognitive Methods in Situation Awareness and Decision Support*, 2013: 212-219.
- [82] Yager R R. Generalized OWA Aggregation Operators[J]. *Fuzzy Optimization and Decision Making*, 2004, 3(1): 93-107.
- [83] Green B, Prince D, Busby J, et al. The Impact of Social Engineering on Industrial Control System Security[C]. *The First ACM Workshop on Cyber-Physical Systems-Security and/or Privacy*, 2015: 23-29.
- [84] Abdo H, Kaoouk M, Flaus J M, et al. A Safety/Security Risk Analysis Approach of Industrial Control Systems: A Cyber Bowtie - Combining New Version of Attack Tree with Bowtie Analysis[J]. *Computers & Security*, 2018, 72: 175-195.
- [85] Motzek A, Möller R. Context- and Bias-Free Probabilistic Mission Impact Assessment[J]. *Computers & Security*, 2017, 65: 166-186.
- [86] Li Z T, Lei J, Wang L, et al. A Data Mining Approach to Generating Network Attack Graph for Intrusion Prediction[C]. *Fourth International Conference on Fuzzy Systems and Knowledge Discovery*, 2007: 307-311.
- [87] Xia C M, Tian J, Li E Q, et al. An Efficient Tool for Industrial Control System Security Analysis[C]. *2016 IEEE 14th Intl Conf on Dependable, Autonomic and Secure Computing, 14th Intl Conf on Pervasive Intelligence and Computing, 2nd Intl Conf on Big Data Intelligence and Computing and Cyber Science and Technology Congress*, 2016: 424-427.
- [88] Wang H, Chen Z F, Zhao J P, et al. A Vulnerability Assessment Method in Industrial Internet of Things Based on Attack Graph and Maximum Flow[J]. *IEEE Access*, 2018, 6: 8599-8609.
- [89] Poolsappasit N, Dewri R, Ray I. Dynamic Security Risk Management Using Bayesian Attack Graphs[J]. *IEEE Transactions on Dependable and Secure Computing*, 2012, 9(1): 61-74.
- [90] Huang L N, Zhu Q Y. Analysis and Computation of Adaptive Defense Strategies Against Advanced Persistent Threats for Cyber-Physical Systems[C]. *Decision and Game Theory for Security*, 2018: 205-226.
- [91] Zhang Q, Zhou C J, Xiong N X, et al. Multimodel-Based Incident Prediction and Risk Assessment in Dynamic Cybersecurity Protection for Industrial Control Systems[J]. *IEEE Transactions on Sys-*

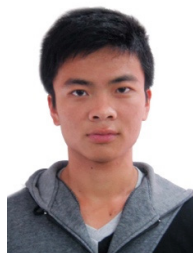
- tems, Man, and Cybernetics: Systems, 2016, 46(10): 1429-1444.
- [92] Li Y M, Voos H, Rosich A, et al. A Stochastic Cyber-Attack Detection Scheme for Stochastic Control Systems Based on Frequency-Domain Transformation Technique[C]. *Network and System Security*, 2014: 209-222.
- [93] Caselli M, Zambon E, Kargl F. Sequence-Aware Intrusion Detection in Industrial Control Systems[C]. *The 1st ACM Workshop on Cyber-Physical System Security*, 2015: 13-24.
- [94] Zimba A, Wang Z S, Chen H S. Multi-Stage Crypto Ransomware Attacks: A New Emerging Cyber Threat to Critical Infrastructure and Industrial Control Systems[J]. *ICT Express*, 2018, 4(1): 14-18.
- [95] M. Antonakakis, T. April, M. Bailey, et al. Understanding the Mirai Botnet[C]. *USENIX Security Symposium*, 2017: 1093-1110.
- [96] P. F. Roberts. Zotob, PnP Worms Slam 13 DaimlerChrysler Plants. Eweek. <https://www.eweek.com/security/zotob-pnp-worms-slam-13-daimlerchrysler-plants>, July, 2019.
- [97] McLaughlin S, Konstantinou C, Wang X Y, et al. The Cybersecurity Landscape in Industrial Control Systems[J]. *The IEEE*, 2016, 104(5): 1039-1057.
- [98] K. Thomas. Hackers Demo Jeep Security Hack. Welivesecurity. <https://www.welivesecurity.com/2015/07/22/hackers-demo-jeep-security-hack/>, July, 2019.
- [99] Dai J, Sun X Y, Liu P. Patrol: Revealing Zero-Day Attack Paths through Network-Wide System Object Dependencies[C]. *Computer Security-ESORICS 2013*, 2013: 536-555.



周明 于 2017 年在中国科学技术大学软件工程专业获得硕士学位。现在中国科学院大学通信与信息系统专业攻读博士学位。研究领域为工控系统安全。研究兴趣包括: 实时操作系统、动态软件更新。
Email: zhouming@iie.ac.cn



吕世超 于 2018 年在中国科学院大学信息安全专业获得工学博士学位。现任中国科学院信息工程研究所第四研究室高级工程师。研究领域为物联网安全、工业控制系统安全。研究兴趣包括: 工控入侵诱捕、工控态势感知。Email: lvshichao@iie.ac.cn



游建舟 于 2015 年在厦门大学电子信息工程专业获得学士学位。现在中国科学院大学通信与信息系统专业攻读博士学位。研究领域为工控安全、物联网安全。研究兴趣包括: 工控蜜罐设计、大数据分析。
Email: youjianzhou@iie.ac.cn



朱红松 于 2009 年在中国科学院大学计算技术研究所获得博士学位。现任中国科学院信息工程研究所研究员。主要研究方向包括物联网安全、网络攻防、安全大数据分析。Email: zhuhongsong@iie.ac.cn



石志强 于 2001 年在中国科学院软件研究所计算机应用技术专业获得工学博士学位。现任中国科学院信息工程研究所正研级高级工程师。研究领域为工业控制系统安全、嵌入式固件脆弱性分析。
Email: shizhiqiang@iie.ac.cn



孙利民 于 1998 年在国防科学技术大学计算机体系结构专业获得工学博士学位。现任中国科学院信息工程研究所研究员。研究领域为物联网安全、工业控制系统安全。研究兴趣包括: 工控入侵诱捕、工控态势感知。Email: sunlimin@iie.ac.cn