通过协调研究项目改进计算机安全异常检测技术

文/Rodney Busquim e Silva 和 Andrea Rahandini

识别控制关键安全和安保功能的计算机系统运行中的异常情况，需要大量的专门知识，而且需要对所需的行动进行测试、分析和修正，从而加以完善。

“异常检测在早期评估针对核设施和辐射设施计算机系统的可能威胁方面发挥着重要作用。”原子能机构核安保司信息管理处处长Scott Purvis说，“通常情况下，异常检测技术基于人工智能应用，如机器学习、统计型或知识型方法或其他技术。这类技术用于识别与预期网络通信或过程测量存在的偏差，这可能是显示入侵者绕过计算机防御系统的第一个指标，并能够提供对网络攻击的实时检测。

这些技术很重要，因为能力极强的恶意行为者可能会引入恶意软件，损害数字系统的安全或安保功能，同时伪造从传感器和指示器发送到操作员的数据。这意味着操作员可能没有意识到恶意活动的发生，最初会根据控制室显示的内容做出反应，有可能被误导而采取错误行动。只有通过自动检测这种网络攻击中最小的异常情况，才能正确地通知操作员。

为了应对这一重要工作领域和其他计算机安全挑战，原子能机构在2016年启动了一项专门协调研究项目。

通过协调研究项目进行研究和发展是原子能机构为促进核安保加强计算机安全活动不可或缺的一部分。这些项目产生了一系列研究和可操作结论，补充了原子能机构正在进行的努力，从而加强各国预防、检测和应对有可能直接或间接影响核设施和辐射设施安全和安保的计算机安全事件以及在发生这类事件后进行恢复的能力。

“敌手变得越来越复杂，他们的网络能力对开发异常检测工具提出了越来越多的挑战，”Purvis说，“开发异常检测技术需要获得现实且实物一致的网络和电厂流程数据，以训练和测试检测模型。”

“我们开发并使用ANS模拟器来生成一个数据库，用于训练我们的机器学习模型，并评价其效率。原子能机构这项协调研究项目联合国际合作伙伴一起开展研究，创造了这一领域的新知识。”

—巴西圣保罗大学理工学院教授Ricardo Marques

用于建立能力的网络攻击情景

题为“加强核设施计算机安全事件分析”的2016年协调研究项目产生了重要成果，例如，成功地进一步研究出有针对性的工具和技术，而以前，如果不暴露核设施和辐射设施的敏感信息，就不可能对这些工具和技术进行研究。

由来自13个国家和17个组织的研究人员组成的协调研究项目团队开发了一个称为“亚舍拉”（Asherah）核电厂的虚构设施，圣保罗大学以该设施为基础开发了一个模拟器（ANS）。他们共同开发了核设施内的真实网络攻击情景。有了这些网络攻击情景，就可以探索和评估计算机安全措施的有效性，以及数字资产遭到破坏的潜在操作后果。此外，该团队还致力于数据收集和分析，以及网络攻击检测技术的开发和测试。

“我们开发并使用ANS模拟器来生成一个数据库，用于训练我们的机器学

圣保罗大学根据“亚舍拉”虚构核电厂设施开发了一个模拟器。（图/国际原子能机构）

习模型，并评价其效率。原子能机构这项协调研究项目联合国际合作伙伴一起开展研究，创造了这一领域的新知识。”巴西圣保罗大学理工学院教授Ricardo Marques说，“协调研究项目参与者之间的合作对于验证所做的工作至关重要。”

此外，这项协调研究项目的成果还被用于大量不同学科的研究生和研究人员的持续教育和培训。这进一步加强了研究和努力，以不断提高核设施和辐射设施的计算机安全。

“我作为博士生的部分研究就是利用ANS模拟器及其人机界面进行的，该界面使用户能够观察模拟器并与模拟器交流，是在原子能机构协调研究项目中开发的。”来自中国清华大学的博士生Si Wen说，“我进行了异常检测技术的研究，ANS模拟器对于产生必要的数据来训练和评估针对核电厂开发的检测算法至关重要。如果没有所有参与研究机构之间的合作以及协调研究项目团队开发的工具，我就不可能进行关于核电厂数字系统网络安全的博士研究，”她补充说。

协调研究项目的成果包括ANS模拟器、工具和导则，可供世界各地感兴趣的研究机构使用，可以通过有关国家主管机构向原子能机构提交申请表获得，申请表可在原子能机构“核安保信息门户”下载。

最近在2023年，原子能机构启动了一个题为“加强辐射探测系统计算机安全”的新协调研究项目，旨在研究改进辐射探测设备计算机安全的方法和技术。来自11个国家的12个组织（包括国家实验室、大学和国家研究机构）参与了这个新协调研究项目，计划开展的研究项目将涉及诸如云计算等新兴数字技术的应用，并继续探索和开发创新型异常检测技术。