网络安全的新威胁及新检测与防御思路

关键词：人工智能安全　物联网安全　安全切面

特邀编辑：谭晓生
北京赛博英杰科技有限公司

网络安全无疑是近几年计算机行业持续关注的热点之一。从2013年网络安全公司Mandiant的APT1报告[1]，到2016年美国大选民主党全国委员会（DNC）竞选邮件泄露事件，2017年WannaCry勒索蠕虫全球爆发，再到2020年Zoom安全漏洞事件、SolarWinds供应链攻击等，网络安全事件不时牵动着人们的神经，“没有网络安全，就没有国家安全”已经是共识。

2016年以来，我国政府一方面密集出台网络安全方面的法律法规，通过“合规性”来推动网络安全建设，一方面通过组织实网攻防演习，真攻真防来检验关键信息基础设施的网络安全防御能力。这套组合拳不仅使社会对网络安全的重视程度有所提高，而且带来了网络安全研究、网络安全产品创新的蓬勃发展。

随着全社会的数字化转型，移动互联网、物联网、工业互联网、人工智能这些新的应用领域的兴起，网络安全的研究领域也在不断扩展。

基于深度学习的人工智能技术的崛起，在人脸识别认证、语音识别、广告推荐、疾病诊断、自动驾驶等领域都有非常成功的应用，用人工智能技术帮助识别网络安全威胁、提高网络安全运营自动化水平也是网络安全领域研究的重点方向之一，但人工智能系统最终也是以软件形式实现，具有脆弱性，已经成为网络攻击的目标。

李康教授团队是国际上最早开始对AI系统的安全性做研究的团队之一，2017年下半年所报告的人工智能系统漏洞获得了十多个CVE编号[2]。李康教授所在百度安全团队胡智圣等人撰写的《ASF：模糊测试技术在AI Safety的应用探索》介绍了百度在自动驾驶业务背景下，用模糊测试（Fuzzing Test）技术对AI承载层进行漏洞挖掘的实践。

薛峰、韦韬撰写的《AI安全的演变：从风险到威胁》则从AI数据层和模型层介绍了对AI系统进行攻击的方法，讲述了数据投毒攻击、对抗攻击和模型窃取三种典型的攻击场景，并提出“安全的本质是对抗，威胁对抗核心三要素是对手、资产和对抗体系”的观点，以及解决人工智能系统安全性的一些方法，比如对攻击对手建模，AI赋能的资产管理，长期进行基于体系的对抗等。

绿盟科技创新中心总监刘文懋撰写的《人工智能在网络安全领域的应用现状》，从人工智能赋能网络安全的角度讲述了人工智能技术应用于网络安全所

[1] 一份关于中国黑客攻击的报告，参阅 https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf。

[2] CVE的英文全称是“Common Vulnerabilities & Exposures”，即通用漏洞披露。CVE相当于一个字典表，为广泛认同的信息安全漏洞或者已经暴露出来的弱点给出一个公共的名称，成为安全信息共享的“关键字”。

面临的挑战：攻击者绕开检测特征而产生漏报，概念漂移造成多场景检测率低，溯源图依赖爆炸造成还原攻击路径困难。然后介绍了人工智能在 Webshell 检测、加密流量识别、AI 辅助安全运营中的应用，并对未来人工智能在网络安全上的应用进行了展望。

浙江大学教授徐文渊撰写的《智联网传感器安全综述：机理、攻击和防护》则转换了一个攻击角度：传感器是物联网与实体环境交互连接的纽带，针对传感器的换能攻击可以干扰物联网的正常工作。文章介绍了传感器换能工作机理、攻击方法与防护方法。

2020 年全球新冠大流行，反倒加速了世界数字化转型的速度，从居家隔离造成电商的繁荣，居家办公造成视频会议业务的 SaaS 软件被广泛接纳，到企业追求更高的自动化生产能力，大型数字化业务复杂性呈爆炸趋势，过去运行在隔离网络中的系统也被迫通过互联网连接起来。网络空间安全保障面临的最大挑战也是这种复杂性爆炸。蚂蚁集团副总裁韦韬撰写的《安全平行切面：我们要改变什么，我们要建设什么》提出了“安全平行切面”概念，提出“业务部署维度与安全部署维度做到正交融合——两者既能融合为一体，又能独立解耦，各自独立发展，而不是绑在一起演进”，给出了一种解法，通过安全平行切面解决感知覆盖、应急攻防、治理与布防的矛盾。

本期专题的五篇文章中有三篇讲述新的网络攻击面：人工智能系统与物联网传感器，两篇讲述防护技术和理念的提升：人工智能赋能网络安全，以及通过安全平行切面方法实现业务与安全既融合，又能解耦合。网络安全面临的新威胁层出不穷，防御思想与理念也需要不断创新，期望本期的几篇文章对大家有所启发。 ■

谭晓生

CCF 杰出会员，CCF 副秘书长，*CCCF* 专题编委。北京赛博英杰科技有限公司 CEO。主要研究方向为网络空间安全、云计算与大数据等。

sztanxs@gmail.com

（本期专题责任编委：**谭晓生**）