Contents lists available at ScienceDirect

Engineering

journal homepage: www.elsevier.com/locate/eng

Editorial

网络安全的新领域

方滨兴[a,b,c], 任奎[d], 贾焰[e]

[a] China Electronics Corporation, Beijing 100846, China
[b] Guangzhou University, Guangzhou 510006, China
[c] Beijing University of Posts and Telecommunications, Beijing 100876, China
[d] University at Buffalo, State University of New York, Buffalo, NY 14228, USA
[e] National University of Defense Technology, Changsha 410073, China


方滨兴


任奎


贾焰

网络安全技术是一种特殊的伴生技术，它为其所服务的底层应用而开发。随着这些底层应用变得越来越互联、普及和智能化，安全技术在当今社会也变得越来越重要。近几年来，我们见证了云计算、边缘计算、物联网（IoT）、人工智能（AI）、工业4.0、大数据以及区块链技术等新兴领域的尖端计算和信息技术的不断普及。虽然这些技术具有巨大的影响潜力，但它们也带来了巨大且不可避免的安全挑战。观察表明，安全事件在数量和规模上都迅速增长，大多数尖端技术固有地伴随着一系列的安全和隐私漏洞。因此，为这些新技术的用户提供可以保障安全和隐私感知环境的高质量服务成为一项非常紧迫的任务。随着网络研究的前沿扩展到未开发的领域，这些新兴技术的特征使其难以套用传统的安全案例。因此，识别这些新兴技术的新特性，仔细检查其所需要的新安全需求，然后将它们正确地整合到开发过程的早期阶段是至关重要的。

为了赶上现代科学和商业应用中所涉及数据量的爆炸式增长，工程实践中对于计算和存储能力的需求促成了云计算技术的发展。在这样的背景下，云计算作为一种整合大量计算资源并提供经济廉价在线服务的商业模式，对资源有限的云客户是非常便利的。尽管这种新技术前景广阔，但其特定特征也可能导致前所未有的安全问题，进而限制了它的广泛应用。这其中，缺乏数据隐私保护被视为云计算的主要安全问题之一，尤其是对专有数据或高度敏感的数据记录而言。不仅如此，使问题变得更为棘手的原因还在于传统加密技术导致的数据质量的损失，即损害数据的原始功能，如关键字搜索和数学计算等。解决这些安全挑战的潜在研究方向包括通过创新性数据加密方法将密文域操作的功能进一步加强以支持更为复杂的应用程序，与现有方法相比，这种方法可以提供更强大的安全保证，以及实际中更加高速的运行效率。

互联网的另一个重要未来方向是物联网，其中，各种形式的互连物理设备（通常包括嵌入式电子设备、软件、传感器、执行器等）共同执行复杂的传感和计算任务，并提供前所未有的服务。将物联网融入我们的生活将彻底改变人们与物理世界的互动方式，并将为医疗保健、运输和制造等领域带来巨大的好处。但是，物联网的兴起也引发了对网络攻击威胁的越来越多的关注。不断增长的各种类型的物联网互联设备为敌手提供了巨大

英文原文: Engineering 2018, 4(1): 1–2
引用本文: Binxing Fang, Kui Ren, Yan Jia. The New Frontiers of Cybersecurity. *Engineering*, https://doi.org/10.1016/j.eng.2018.02.007

而广泛的网络攻击入口。此外，物联网设备的异构接口、系统和硬件的组合对保护这些设备同样构成了重大挑战。未能保护物联网设备可能会导致攻击者访问私人信息和（或）对设备进行未经授权的控制。

通信协议的多样化也增加了物联网设备可能遭受的威胁。目前使用的各种无线接入技术不仅增加了物联网的复杂性，还暴露出了大量的漏洞。这些漏洞的存在可能允许入侵者嗅探物联网设备生成的数据或危害设备本身。为了解决这个问题，研究人员必须提供解决方案来保护联网的物联网设备，使用户能够在各种设备上执行安全策略，并能更好地控制和管理敏感信息，减轻更新设备所带来的压力。

新一代计算机科学发展的核心工具——人工智能为网络安全带来了一系列机遇和挑战。一方面，从网络钓鱼检测和监控系统到基本密码算法等的安全技术在人工智能的协作下变得越来越强大和智能化。例如，传统的垃圾邮件检测模型正在通过与严格的网络钓鱼分析相关的专用机器学习模型进行更新，这些模型的检测准确率可以达到99％以上。使用人工智能代替视频分析员可以提高效率和准确性，其威胁感知能力也可以得到提升。此外，随着生成对抗网络（GAN）的出现，人工智能可能在不久的将来革新密码技术。人工智能带来的所有安全技术进步都归功于其自我学习和自我增强能力。人工智能能够挖掘和学习各种类型的数据，如垃圾邮件、语音消息以及视频，然后更新自动检测/防御系统。持续的自我培训将继续增强以人工智能为核心的安全系统的性能，包括其稳定性、准确性、效率和可扩展性。因此，人工智能具有巨大的潜力来改变未来的安全态势。

另一方面，人工智能也在拓展黑客能力的界限。由人工智能驱动的自主黑客攻击机可以制作敏感信息并发现计算机系统中的漏洞，从而使与黑客对抗变得更加困难。更糟糕的是，人工智能能够从大量如个人偏好一类的看似不敏感的数据中推导学习敏感信息。这些事实使我们相信，装备了人工智能武器的黑客将进行更复杂也更隐蔽的自动配对攻击，这将需要我们进一步开发更为有效的检测和应对技术。

若从另一个角度考虑人工智能与网络安全之间的相互作用，可以发现人工智能技术本身也正面临着对抗环境中的各种安全挑战。某些任务的机器学习模型被认为是宝贵的知识产权，通常需要经过大量的数据与长时间的机器学习才能获得。不仅如此，模型还可能依赖敏感的培训数据，或可能在安全应用程序中运行。然而，在没有训练数据或模型参数的先验知识的情况下，机器学习模型可能被窃取。这种窃取的受害者就包括了一些在线机器学习服务的提供方，如BigML和亚马逊机器学习。此外，即使是训练数据也可以通过利用随测试数据预测显示的置信度值来推断。例如，敌手可以反向推断与模拟用于面部识别模型的训练数据中使用的某部分图像。通过这种方式，可以获取人工智能训练过程中输入数据的信息乃至数据集中参与者的身份。因此，保护机器学习模型和训练数据亦将成为一个关键且具挑战性的问题。

此外，机器学习模型，特别是深度神经网络，可能会被人类肉眼察觉不到的对抗样本所迷惑。以图像识别为例，只要敌手在图像上添加特殊的肉眼不可见的干扰信息，深度神经网络就可能将人眼看起来像鸟儿的图像识别为船。这种脆弱性成为人工智能在自动驾驶汽车和计算机辅助诊断等安全性要求非常高的场景中应用所面对的关键风险。因此，不久的将来在有效检测对抗样本方面需进行大量的研究工作。

网络安全在过去十年左右一直是一个受到持续关注的热点领域。不断发展的安全技术本质上是由新生技术的成功推动的，如云、物联网、人工智能等新技术的不断出现。随着这些崭新应用所面对的不断变化的安全威胁的出现，网络安全技术的前沿也不断拓展。新的网络安全技术需要将网络、计算系统、安全理论以及工程基础作为多学科课题进行整体研究与实践。通过调查实际应用的系统功能和安全需求，我们最终可以解决不断出现的具有高度挑战性的全新安全问题并共同构建真正安全的网络空间。通过本期网络安全专题，我们希望将安全、隐私和计算领域的研究人员、开发人员和实践者聚集在一起，共同塑造网络安全的未来。

致谢

这项工作得到了国家自然科学基金（U1636215, 61572492,61650202,61772236和61372191）和国家重点研发计划（2016YFB0800802, 2016YFB0800803, 2016YFB0800804, 2017YFB0802204, 2016QY03D0601, 2016QY03D0603和2016YFB0800303）的部分支持。