Contents lists available at ScienceDirect

Engineering

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

Topic Insights

网络安全研究——成功的数字化未来的关键

Jackie Craig

Fellow of the Australian Academy of Technological Sciences and Engineering, Australia

1. 引言

通过掀起数字变革，科学技术展现出了其深刻影响我们生活方方面面的能力，并在网络空间的虚拟世界中发挥出来[†]。网络空间提供了其他空间难以企及的连通性和全球影响力，并已经成为了社会和经济福祉的核心。我们对网络空间的依赖正在增加，与此同时，随着网络威胁变得更多变、严重、持久，并且难以发现和反击，网络空间在有害事件面前也显得更加脆弱。因此，网络安全在所有数字国家都应该被置于极高的优先级，现在很多国家都有国家网络安全战略（参见文献[1,2]）。

2. 网络依赖

网络空间是一个动态的、不断发展的环境，为我们提供了无法通过其他方式实现的功能。现在，政府、组织和个人依靠网络空间来交流、协作、提供或使用服务，而且电子商务、电子学习、电子研究和电子健康等概念也已成为常态。

带有嵌入式控制器的设备正在不断增加，我们正处于物联网的曙光之中，预计到2020年将有200亿台设备连接到网络[3]。包含远程监控和管理关键基础设施、公共建筑、交通、商业和家庭的愿景的智慧城市概念正在加速发展。现在，用于家庭的智能电表、与移动电话连接的家庭安全系统、无人驾驶汽车已经出现，智慧城市计划也被提出（参见文献[4]）。

3. 脆弱性、威胁和网络安全研究

网络空间在扩张和发展的同时，也在许多因素的影响下变得越来越脆弱[5]。网络、设备和用户数量的增加导致了攻击面不断扩大。日益增长的相互关联性和相互依赖性显著增加了风险，即系统的某个部分出现故障可能导致级联和远期效应。网络空间增加的复杂性和外包使系统难以实现完整可视性和安全性。其他重要的风险因素包括遗留系统、不良网络卫生对网络技术供应链的控制不足以及训练有素的网络安全专业人员不足等。

网络威胁是持续且不断演变的。未来，随着硬件威胁（如硬件木马）范围的扩大，网络攻击从基于代码的攻击转变为对数据完整性和业务流程的攻击，以及系统性影响的出现，风险将会不断提升。

先前的规律证明，威胁-对策周期对网络攻击者而言是有利的。而研究对于提供洞察力、工具和途径来加强网络安全方法和能力至关重要，不仅要改善我们的现状，还要确保安全和有恢复能力的数字化未来。网络安全研究大致可以分为3个领域：系统、信息和人员。

4. 系统

概念框架对于在复杂的、相互关联、相互依存和适应性系统中捕捉和解决网络安全的关键要素而言具有极高的实际价值。在本期网络安全专题中，杨小牛等讨论

[†] 本文中，网络空间被定义为由互联网、通信网络、计算机系统和信息物理（嵌入式控制器）系统组成的一个相互连接的全球域。

英文原文: Engineering 2018, 4(1): 9–10
引用本文: Jackie Craig. Cybersecurity Research—Essential to a Successful Digital Future. *Engineering*, https://doi.org/10.1016/j.eng.2018.02.006

了这样一种框架。

无论使用何种框架，都必须建立在不能保证完全安全的系统的前提下，而重点必须放在确保面对有害网络事件时的任务恢复能力上。这需要以对任务目标的共同理解、共同的综合态势感知和协调一致的响应为基础的全系统方法作为支撑。

全面的情景意识是从体系结构、脆弱性、潜在威胁、网络安全政策、活动和系统状态数据中形成的。这是一个大数据问题，而为了满足网络安全的实时要求，有必要进行研究，为这些数据的自动摄取、处理、融合、分析和显示提供工具和技术。

同样，研究对协调行动而言也是举足轻重的，因为它提供了诸如决策辅助工具、支持有效协作的工具和人工智能（AI）等功能，以此为行动方案提供建议。

总之，我们可以期待对AI和自主性的研究不断深入，因为这些将在整个系统架构中出现，并被用来加强人们拦截和响应先进、持久的网络威胁的能力。

5. 信息

信息是数字世界的基础资源，因此，必须保持信息可用性、完整性和隐私的安全。由于多个数据泄露实例的出现，隐私最近成为一个值得注意的话题。在那些数据泄露的实例中，许多用户的个人信息已经被公开发布。人们经常在网上分享个人信息，尤其是照片。他们还定期与在线提供商共享信息（无论是有意还是无意），而供应商使用这些信息在推荐系统中个性化他们的服务。分析共享信息可以用来窥探个人偏好、社交网络、生活方式选择和生活模式。因此，保护共享信息的重要性远远超出了该信息的内在价值。

研究照片共享的隐私保护技术的范围包括了从操纵图像到帮助用户控制传播。它包括诸如对图像部分进行端到端加密、带标签的照片管理方案以及利用人际关系印象管理方案推荐分享策略等方法（李凤华等，本期网络安全专题）。

同样，一些针对推荐系统中的隐私保护的方法和策略正在研究中。这些方法根据推荐系统所使用的技术而变化，王聪等在本期网络安全专题中对此进行了阐述。

在我们对隐私的关注中，数据的完整性是不容忽视的。信息是我们所有决策和行动的基础，而数据完整性的缺陷可能对系统稳定性和业务连续性造成非常严重的后果。包括网络数据、流量流、协议和用户数据在内的所有数据都受到完整性要求的限制。完整性测试包括一些较为简单的过程，例如检查缺失值并确定值是否位于特定范围内。而检查真实图像等复杂数据的完整性则较为困难，需要使用多学科技术来检查其真实性。林祥等在本期网络安全专题中对这一领域进行了回顾。

6. 人员

人员是良好网络安全环境的一个关键要素。无论网络安全措施如何，无论是通过恶意行为还是失当的网络安全应对措施，人员通常都是网络安全失败的原因。理解诸如认知功能、动机、行为和影响等在内的人类特征对维护和改善网络安全至关重要[6]。例如，对认知功能的理解有助于提升重要网络安全信息的可视化水平；同样，关于动机和行为的知识可以为网络安全政策的实施提供指导，以提高其成功的可能性。

社会影响力分析提供了对个人和群体如何受其他人影响的内在联系，这也是当前活跃的研究领域之一。有许多模型可以描述和预测社会影响力（李侃等，本期网络安全专题）。这些模型可以提供关于谁拥有最强大的影响力、谁最有可能受到影响以及影响以何种方式作用的相关信息。在网络安全领域，这些信息是非常有用的工具。例如，理解影响力及其作用方式可以帮助提高个体对网络钓鱼——一种非常普遍成功且越来越复杂的攻击手段——的抵御能力。

人们日渐认识到研究网络安全问题的重要性。这项研究将塑造未来的系统设计、网络政策和在线行为，并将推动人为因素成为网络安全架构的组成部分。

7. 总结

科学技术的进步为我们提供了一个数字世界，而我们正在越来越依赖这个世界。随着网络空间的扩张和变化，它容易受到不断发展和持续的网络威胁的攻击。对网络安全的研究不容忽视，因为这项研究将提供使数字世界成为一个充满活力和安全的地方的解决方案。

References

[1] Her Majesty's Government. National cyber security strategy 2016–2021. London: Her Majesty's Government; 2016.
[2] Cybersecuritystrategy.pmc.gov.au [Internet]. Canberra: Department of the

Prime Minister and Cabinet, Australian Government; [cited 2018 Jan 15]. Available from: https://cybersecuritystrategy.pmc.gov.au.
[3] Nordrum A. Popular Internet of Things forecast of 50 billion devices by 2020 is outdated [Internet]. New York: IEEE Spectrum; c2018 [updated 2016 Aug 18; cited 2018 Jan 15]. Available from: https://spectrum.ieee.org/tech-talk/telecom/internet/popular-internet-of-things-forecast-of-50-billion-devices-by-2020-isoutdated.
[4] Buntz B. The world's 5 smartest cities [Internet]. New York: Informa USA, Inc.; c2018 [updated 2016 May 18; cited 2018 Jan 15]. Available from: http://www.ioti.com/smart-cities/world-s-5-smartest-cities.
[5] Science and Technology for Safeguarding Australia. Future cyber security landscape: A perspective on the future. Canberra: Defence Science and Technology Group; 2014.
[6] Furnell S, Clarke N. Power to the people? The evolving recognition of human aspects of security. Comput Secur 2012;31(8):983–8.