Recent Advances in Securing Networked Systems

Trent Jaeger and **Chengyu Song** | University of California, Riverside

This special issue examines the security challenges in modern networked systems from the perspective of edge devices, core network, and specialized security services and provide guidance in these areas.

Network systems continue to evolve in a variety of ways. While software-defined networking has been around for about 15 years, programmable network approaches continue to emerge, which both create new threats to networked systems and provide a foundation for addressing existing threats. Similarly, the capabilities of edge devices create new challenges for protecting data from remote adversaries and preventing devices being exploited to launch new attacks. Another question is how network defenses that have become commonplace, such as honeypots, may address such challenges or may need to be rethought in these modern networked systems.

> **Programmable network approaches continue to emerge, which both create new threats to networked systems and provide a foundation for addressing existing threats.**

This special issue examines modern network systems from these three perspectives: the network core, the network edge, and the network security mechanisms. The authors have provided a diverse range of perspectives for readers to consider in discovering new research problems in network security as well as assessing proposed security solutions. These articles are also from a variety of sources, including the Army Research Laboratory's Cyber Security Collaborative Research Alliance, on which both of us participated. We hope you enjoy this selection of articles.

Two articles examine security issues at the network edge. Chan and Johnsen[A1] discuss security issues at the edge of tactical networks, particularly reviewing the challenges identified by a recent North American Treaty Organization report. Shi et al.[A2] discuss privacy

Digital Object Identifier 10.1109/MSEC.2025.3609985
Date of current version: 10 November 2025

1540-7993 © 2025 IEEE. All rights reserved, including rights for text and data mining, and training of artificial intelligence and similar technologies.

challenges in extended reality devices in edge networks, demonstrating vectors for the leakage of a variety of personal data.

Two articles examine how programmability in the network core may present security issues and present a foundation for effective defenses. Ujcich[A3] discusses the evolution from software-defined networking to the modern version of the programmable network, reviewing attack vectors and potential directions for addressing these vectors. Zhou and Gu[A4] discuss efforts to secure networked systems by leveraging programmable data planes, reviewing efforts for attack detection and mitigation, as well as the issues that limit such approaches.

Two articles examine how modern networked systems impact the future of network defenses, in particular honeypots. Pauley et al.[A5] argue that modern cloud systems reduce the visibility that honeypots have into attacker behaviors, but they also leverage the elasticity of cloud systems to make honeypot deployment more dynamic to improve their utility. Guan et al.[A6] explore the application of honeypots as a defense for Internet of Things systems, applying reinforcement learning techniques to learn how to interact with attackers to uncover malicious activities.

We hope that these articles help inform practitioners about emerging threats as well as opportunities for improving defenses in modern networked systems. ■

Appendix: Related Articles

A1. K. S. Chan and F. T. Johnsen, "Cybersecurity in tactical edge networks," *IEEE Security Privacy*, vol. 23, no. 6, pp. 10–20, Nov./Dec. 2025, doi: 10.1109/MSEC.2025.3610295.

A2. C. Shi, Y. Wang, Y. Chen, and N. Saxena, "Your headset is listening: Motion sensor side-channels and the future of extended reality privacy," *IEEE Security Privacy*, vol. 23, no. 6, pp. 21–31, Nov./Dec. 2025, doi: 10.1109/MSEC.2025.3603109.

A3. B. E. Ujcich, "A systems security approach for emerging programmable network architectures," *IEEE Security Privacy*, vol. 23, no. 6, pp. 32–41, Nov./Dec. 2025, doi: 10.1109/MSEC.2025.3603133.

A4. H. Zhou and G. Gu, "Securing networks with programmable data planes: Opportunities and challenges," *IEEE Security Privacy*, vol. 23, no. 6, pp. 42–50, Nov./Dec. 2025, doi: 10.1109/MSEC.2025.3603621.

A5. E. Pauley, P. Barford, and P. McDaniel, "Clouds are where the (security) action is: Have honeypots been left in the dust?" *IEEE Security Privacy*, vol. 23, no. 6, pp. 51–57, Nov./Dec. 2025, doi: 10.1109/MSEC.2025.3603410.

A6. C. Guan, J. Zhang, G. Cao, T. F. La Porta, and J. C. Acosta, "Learning-based Internet of Things honeypots for cyber deception," *IEEE Security Privacy*, vol. 23, no. 6, pp. 58–65, Nov./Dec. 2025, doi: 10.1109/MSEC.2025.3601986.

Trent Jaeger is a professor in the Department of Computer Science and Engineering, University of California, Riverside, CA 92521 USA. His research interests include systems security and software security. Jaeger received a Ph.D. in computer science and engineering from the University of Michigan, Ann Arbor. This author is a Fellow of IEEE. Contact this author at trentj@ucr.edu.

Chengyu Song is an associate professor in the Department of Computer Science and Engineering, University of California, Riverside, CA 92521 USA. His research interests include system security, program analysis and verification, and operating systems. Song received a Ph.D. in computer science from Georgia Institute of Technology. He is a Member of IEEE. Contact him at csong@cs.ucr.edu.