Communications of the ACM

2025-03	Exploiting Cross-Layer Vulnerabilities: Off-Path Attacks on the TCP/IP Protocol Suite
2025-02	Questioning the Criteria for Evaluating Non-Cryptographic Hash Functions
	Program Correctness through Self-Certification
	It Is Time to Standardize Principles and Practices for Software Memory Safety
2025-01	Open VPN Is Open to VPN Fingerprinting
	GPTs and Hallucination
2024-12	Confidential Computing or Cryptographic Computing?
2024-11	Human-Centered Cybersecurity Revisited: From Enemies to Partners
	Pitfalls in Machine Learning for Computer Security
2024-04	The Science of Detecting LLM-Generated Text

IEEE Security & Privacy

2025 vol1	The Rise of Cybercrime and Cyber-Threat Intelligence
	Developers: Beware of Timing Side-Channels
2024 vol6	Emerging Paradigms in Wearable Security
	Android Permissions: Evolution, Attacks, and Best Practices
	Adoption Challenges for Cryptographic Protocols
2024 vol5	From Privacy-Invasive Parental Control to Teen-Centric Solutions for Digital Resilience
	AI Code Generators for Security: Friend or Foe?
2024 vol4	Memory Safety

Feel free to propose another topic of your interest
(by E-Mail to peter.schartner@aau.at) **iff** it is covered in
Communications of the ACM, IEEE Security & Privacy or IEEE Computing Edge