1.	Record Nr.	UNINA9911001465803321
	Titolo	Foundations and Practice of Security : 17th International Symposium, FPS 2024, Montréal, QC, Canada, December 9–11, 2024, Revised Selected Papers, Part I / / edited by Kamel Adi, Simon Bourdeau, Christel Durand, Valérie Viet Triem Tong, Alina Dulipovici, Yvon Kermarrec, Joaquin Garcia-Alfaro
	Pubbl/distr/stampa	Cham : , : Springer Nature Switzerland : , : Imprint : Springer, , 2025
	ISBN	3-031-87499-4
	Edizione	[1st ed. 2025.]
	Descrizione fisica	1 online resource (XVI, 416 p. 113 illus., 79 illus. in color.)
	Collana	Lecture Notes in Computer Science, , 1611-3349 ; ; 15532
	Disciplina	005.8
	Soggetti	Data protection Computer engineering Computer networks Data and Information Security Computer Engineering and Networks Computer Communication Networks
	Lingua di pubblicazione	Inglese
	Formato	Materiale a stampa
	Livello bibliografico	Monografia
	Nota di contenuto	-- Critical issues of protecting systems against digital threats, considering financial, technological, and operational implications. -- The Perfect Victim? Family Offices as Targets for Cybercriminals. -- Advanced Real-Time Detection of Cyber Threat Information from Tweets. -- Mitigating spillover effects of ransomware in financial markets: Lessons from the LockBit attacks. -- Exploring Smart Speaker Disclosure and Adoption Intentions: A Privacy Adoption Calculus Perspective. -- ICoSSiuM: an Integrated Communication Security Simulator for Maritime operations. -- Automating and enhancing security mechanisms in software systems and data management. -- Lowering the Barrier: An Automatic Attack Flow Generation Framework for Non-Security Experts. -- An Approach to Determine a System's Behavioural Security Posture. -- Secure Data Traceability for Mobile DataCollectors. -- Toward Automatic Enforcement of Security Patterns in Software Architecture Using Alloy. -- Cybersecurity and AI when

applied to emerging technologies. -- Light-SABRE: A lightweight encrypted data distribution system for Internet of Things. -- Evaluating Large Language Models on Cybersecurity Knowledge and Skills: A Comparative Analysis. -- Drone Anomaly Detection: Dataset and Unsupervised Machine Learning. -- A Tool for Enabling Scalable Automation in Security Control Selection. -- Cybersecurity and Ethics. -- A Systematic Evaluation of Non-SDK Interface Restrictions in Android: Bridging the Gap Between Guidelines and Practice. -- An Approach for Handling Missing Attribute Values in Attribute-Based Access Control Policy Mining. -- Does Gender Matter? Examining and Mitigating Gender Bias in Fake News Detection. -- ProFineLlama: A Prompt and Fine-Tuned Transfer Learning Approach for Multi-Domain Fake News Detection. -- Parametric Automata for Dynamic Access Control Policies. -- Cybersecurity and privacy in connected and autonomous systems for IoT, smart environments, and critical infrastructure. -- Fingerprinting Connected Wi-Fi Devices Using Per-network MAC Addresses. -- Privacy Guard: Empowering Users with Privacy Labels and Intuitive Apps. -- Privacy Guard: Empowering Users with Privacy Labels and Intuitive Apps Substation Automation Security. -- Enhancing Autonomy of Context-Aware Self-Healing in Fog Native Environments. -- Detecting Cyber Attacks on Electric Vehicles Charging Stations. -- New trends in advanced cryptographic protocols. -- Secure Voting Protocol Using Balance Scale. -- Monitoring the execution of cryptographic functions. -- RouterORAM: An O(1)-latency and client-work ORAM.

Sommario/riassunto	This two-volume set constitutes the refereed proceedings of the 17th International Symposium on Foundations and Practice of Security, FPS 2024, held in Montréal, QC, Canada, during December 09–11, 2024. The 28 full and 11 short papers presented in this book were carefully reviewed and selected from 75 submissions. The papers were organized in the following topical sections: Part I: Critical issues of protecting systems against digital threats,considering financial, technological, and operational implications; Automating and enhancing security mechanisms in software systems and data management; Cybersecurity and AI when applied to emerging technologies; Cybersecurity and Ethics; Cybersecurity and privacy in connected and autonomous systems for IoT, smart environments, and critical infrastructure; New trends in advanced cryptographic protocols. Part II: Preserving privacy and maintaining trust for end users in a complex and numeric cyberspace; Intersecting security, privacy, and machine learning techniques to detect, mitigate, and prevent threats; New trends of machine leaning and AI applied to cybersecurity.