
Italy June 30, 2025
Conference Website: https://wtmc.info/index.html

About the Conference

CALL FOR PAPERS

10th International Workshop on Traffic Measurements for Cybersecurity (WTMC 2025)
co-located with
10th IEEE European Symposium on Security and Privacy 2025

Venice, Italy
Monday, June 30th, 2025

WTMC website: https://wtmc.info/index.html

IMPORTANT DATES

February 10, 2025 (AoE, UTC -12): Paper Submission
March 24, 2025: Notification Date
April 7, 2025: Camera-Ready Paper Deadline

Overview

Current communication networks are increasingly becoming pervasive, complex, and ever-evolving due to factors like enormous growth in the number of network users, continuous appearance of network applications, increasing amount of data transferred, and diversity of user behavior. Understanding and measuring traffic in such networks is a challenging yet vital task for network management but recently also for cybersecurity purposes. Network traffic measurement and monitoring can, for example, enable the analysis of the spreading of malicious software and its capabilities or can help to understand the nature of various network threats, including those that exploit user's behavior and other user's sensitive information. On the other hand, network traffic investigation can also help to assess the effectiveness of the existing countermeasures or contribute to building new, better ones. Traffic measurements have been utilized in the area of economics of cybersecurity e.g., to assess ISP “badness” or to estimate the revenue of cybercriminals. Recent research has focused on measurements of fake news and the interplay between misinformation and user engagement in news postings using different online platforms. Additionally, recent studies have explored measurements of generative AI's role in cybersecurity, highlighting its dual potential to bypass security measures in cyberattacks and strengthen defense mechanisms against evolving threats.

The WTMC workshop aims to bring together the research accomplishments provided by researchers from academia and the industry. The other goal is to show the latest research results in the field of cybersecurity and understand how traffic measurements can influence it. We encourage prospective authors to submit related distinguished research papers on the subject of both theoretical approaches and practical case reviews. This workshop presents some of the most relevant ongoing research in cybersecurity seen from the traffic measurements perspective.

The workshop will be accessible to both non-experts interested in learning about this area and experts interested in hearing about new research and approaches.

Topics of interest include but are not limited to:
- Measurements for network incidents response, investigation, and evidence handling
- Measurements of cyber attacks (e.g., DDoS, botnet, malware, and phishing campaigns)

- Measurements for the security of web-based applications and services (e.g., social networking)
- Measurements of the impact and applications of generative AI in cyberdefense and cyberattacks
- Measurements for network anomalies detection
- Measurements for the economics of cybersecurity and privacy
- Measurements of security and privacy for the Internet of Things
- Measurements of Internet censorship
- Measurements of trends in the diffusion of misinformation on social media
- Measurement studies describing the impacts of regulations on cybersecurity and users' privacy (e.g., GDPR)
- Network traffic analysis to discover the nature and evolution of the cybersecurity threats
- Measurements of cyber-physical systems security
- Measurements for assessing the effectiveness of the threats detection/prevention methods and countermeasures
- Novel passive, active, and hybrid measurements techniques and tools for cybersecurity purposes
- Traffic classification and topology discovery tools for monitoring the evolving status of the network from the cybersecurity perspective
- Correlation of measurements across multiple layers, protocols, or networks for cybersecurity purposes
- Machine learning and data mining for analysis of network traffic measurements for cybersecurity
- Novel approaches for large-scale measurements for cybersecurity (e.g., crowd-sourcing)
- Novel visualization approaches to detect network attacks and other threats
- Analysis of network traffic to provide new insights about network structure and behavior from the security perspective
- Measurements of network protocol and applications behavior and its impact on cybersecurity and users' privacy
- Vulnerability measurements and notifications
- Measurements for new cybersecurity settings
- Ethical issues in measurements for cybersecurity
- Reappraisal of previous empirical findings

SUBMISSIONS

Papers will be accepted based on single-blind peer review (3-4 per paper) and should contain original, high-quality work. All papers must be written in English.

Authors are invited to submit short papers (up to 4 pages +2 for appendices/references), regular papers (up to 6 pages +2 for appendices/references), and long papers (up to 10 pages +4 for appendices/references) via EasyChair (https://easychair.org/conferences/?conf=wtmc2025). Reviewers are explicitly not expected to read the appendices while deciding whether to accept or reject the paper.

Papers must be typeset in LaTeX in A4 format (not "US Letter") using the IEEE conference proceeding template we supply eurosp-template.zip (https://eurosp2025.ieee-security.org/eurosp-template.zip). We recommend using LaTeX, and suggest you first compile the supplied LaTeX source as is, checking that you obtain the same PDF as the one supplied. Then, write your paper into the LaTeX template, replacing the boilerplate text. Please do not use other IEEE templates. Failure to adhere to the page limit and formatting requirements can be grounds for rejection.

Submissions must be in Portable Document Format (.pdf). Authors should pay special attention to unusual fonts, images, and figures that might create problems for reviewers. Your document should render correctly in Adobe Reader XI and when printed in black and white.

Submissions failing to conform to the submission guidelines risk rejection without review.

Papers describing cybersecurity measurement studies should include an ethical considerations paragraph, and where applicable reach out to their institutional ethics committee or institutional review board. For guidance see the Menlo Report and its companion document.

Authors are encouraged to share developed software implementations, measurement datasets, simulation models, etc. used in articles allowing other researchers to build upon and extend current results. Authors may include a paragraph about reproducible research.

WTMC allows using generative AI but its usage must be transparently disclosed. Larger content (e.g., sections, figures) must be detailed in the appendix, specifying the AI tool and version used. This ensures clarity about the role of AI in the research process. These guidelines are designed to balance the benefits of AI while maintaining ethical standards. Non-compliance may result in paper rejection.

Submission page: https://easychair.org/conferences/?conf=wtmc2025

Submission of a paper implies that should the paper be accepted, at least one of the authors will register and present the paper at the conference.

Papers accepted by the workshop will be published through IEEE Xplore in a volume accompanying the main IEEE Euro S&P conference proceedings.

ORGANIZING COMMITTEE

Maciej Korczyński, Grenoble Alps University, France
Wojciech Mazurczyk, Warsaw University of Technology, Poland
Pedro Casas, Austrian Institute of Technology, Austria

Topics of Interest

2 topics

Research papers are invited in, but not limited to, the following areas:

- Cybersecurity & Privacy
- Internet of Things & Embedded Systems

Important Dates

Jun 30
Conference Date
June 30, 2025