86th Meeting of the IFIP 10.4 Working Group on Dependable Computing and Fault Tolerance
Gold Coast, Australia, 27th - 30th June 2024

Last updated: 12 June 2024

Workshop on Trustworthy AI Systems and Networks

Co-Chairs:

- Dan Dongseong Kim (The University of Queensland, Australia), email: dan.kim@uq.edu.au
- Domenico Cotroneo (University of Naples Federico II, Italy), email: cotroneo@unina.it
- Guangdong Bai (The University of Queensland, Australia), email: g.bai@uq.edu.au

Program

Day 1: Thu., 27 June 2024 (Location: **Kauri**, Crowne Plaza Surface Paradise)
6:30pm Registration open
7:00pm Welcome Reception

Day 2: Fri., 28 June 2024 (Location: Phoenix room, Crowne Plaza Surface Paradise)
8:00am-8:30am: Welcome Opening

- Introduction to the WG
  (Marco Vieira)
- Introduction to the Meeting and Workshop
  (Domenico Cotroneo, Dan Kim, Guangdong Bai)
- Introduction of members/guests

8:30am-10:30am: Session 1 – Security, Safety and Fault Tolerance of AI systems.
(Rapporteur: Ilir Gashi)

- Safe and Secure AI/ML-driven Autonomous Vehicles? Not anywhere near yet …
  (Paulo Esteves-Veríssimo, KAUST, Saudi Arabia)
- On Fault Tolerance of AI Systems
  (Long Wang, Tsinghua University, China)

10:00am-10:30am: Discussion
10:30am-11:00am: Coffee Break

11:00am-1pm: Session 2 – AI Security I
(Rapporteur: Karthik Pattabiraman)

- Building Trust in AI Code Generators: A Focus on Robustness and Security
  (Domenico Cotroneo, Università degli Studi di Napoli Federico II, Italy)
- Securing AI Models: Strategies to Prevent Stealing Attacks
  (Sangkyun Lee, Korea University, Republic of Korea)

12:30pm-1pm: Discussion
1:00pm-2:30pm: Lunch (Location: Relish restaurant, Crowne Plaza Surface Paradise)
3:30pm Coffee Break
4:00pm-6pm: Session 3 – AI applications
(Rapporteur: Jiangshan Yu)

- When Green Computing Meets Performance and Resilience SLOs
  (Ravishankar K. Iyer, UIUC, USA)
- Blockchain Room of Requirements (BR^2): an LLM-Enhanced Simulator for Blockchain Protocols
  (Cong Wang, City University of Hong Kong, Hong Kong)

5:30pm-6pm: Discussion
Dinner on Friday is on your won.

Day 3: Sat., 29 June 2024 (Location: Phoenix room, Crowne Plaza Surface Paradise)
8am-9:30am: Session 4 – AI Security II
(Rapporteur: Xavier Defago)

- Path-Sensitive Abstract Execution for Software Vulnerability Detection
  (Yulei Sui, University of New South Wales, Australia)
- Towards Securing Graph Neural Networks in MLaaS
  (Xingliang Yuan, The University of Melbourne, Australia)

9:30am-10am: Discussion
10:00am-10:30am: Coffee Break
10:30am-12pm: **Workshop Wrap-Up (Rapporteurs' summary of the talks)**
12pm-6pm: half day excursion (winery tour with lunch)
7pm: banquet at the workshop hotel (Location: Horizon Dining, Crowne Plaza Surface Paradise)

Day 4: Sun., 30 June 2024 (Location: Phoenix room, Crowne Plaza Surface Paradise)
8:30am-10am: Session 5 - Research reports
10am-10:30am: Coffee break
10:30am-12:30pm: Business meeting (non-member and then members only)
12:30pm-2pm: Lunch

End of 86th IFIP WG 10.4 Meeting