Digital Overground

Cybersecurity and Privacy Institute Student Newsletter

Welcome back! For our first newsletter of 2024, we would like to wish you the best of luck in your Winter term academics, as well as encourage you to consider the importance of non-academic interests as part of your school/life balance. We are all aware of the pressures and expectations that accompany our university careers, and it is important to make the time to decompress and have a little fun!

For your mental and physical health, getting away from the laptop and blowing off some steam is critical; burnout is real.

Remember, community is a major part of school and life; spend some time with people who understand what you're dealing with and always ask for and offer support when it is needed.

If we don't get there together, we don't get there at all!

For those who are interested in contributing to this newsletter, please email us at CPI Students <cpi.students@uwaterloo.ca> we need the support and welcome the input!

Upcoming Events

Medieval Times at CMH

Cooking Show at Fed Hall

Lunar New Year at REV

Valentine's Day at CMH

#MonsterMasterclass: Free Grant-Writing and Networking Workshop for Artists

Drag It UP! at UP Lounge

Black History Month Launch 2024:Black History, Black Heritage, Black Future

GRADflix Showcase

Indigenous Speakers Series presents Chelsea Vowel

Student Support and Resources

Campus Wellness and Counselling Services

CPI for Students

Current Students Pathways

CPI Undergraduate Award

CPI Excellence Graduate Scholarship

The Vector Digital Talent Hub

Research

Flow Correlation Attacks on Tor Onion Service Sessions with Sliding Subset Sum

Daniela Lopes, Jin-Dong Dong, Pedro Medeiros, Daniel Castro, CPI Member Diogo Barradas, Bernardo Portela, Jo˜ao Vinagre, Bernardo Ferreira, Nicolas Christin, Nuno Santos

Meta-ATMoS+: A Meta-Reinforcement Learning Framework for Threat Mitigation in Software-Defined Networks

Hauton Tsang, Mohammad A. Salahuddin, Noura Limam, CPI Member Raouf Boutaba

NetShuffle: Circumventing Censorship with Shuffle Proxies at the Edge

Patrick Tser Jern Kon, Aniket Gattani, Dhiraj Saharia, Tianyu Cao, CPI Member Diogo Barradas, Ang Chen, Micah Sherr, Benjamin E. Ujcich

Accelerating the Transition in the Context of Sustainable Development

Multiple Authors inc. CPI Member Sarah Burch

Open Calls

NVIDIA Graduate Fellowship Program

The Vector Digital Talent Hub encourages students to create profiles on their website to apply for a variety of employment opportunities. | Vector Institute

ICITST 2023 : International Conference for Internet Technology and Secured Transactions

In the Media

- **Podcast of the Month:** Cybersecurity Today – This episode reports on ransomware attacks, an undetected attack on a VMware hole and more
- Cyber Security Paths - The LAST Roadmap You'll Ever Need
- Hacking Tools (with demos) that you need to learn in 2024
- Microsoft Says Russian Gov Hackers Stole Email Data From Senior Execs
- Apple Ships iOS 17.3, Warns of WebKit Zero-Day Exploitation
- Outsmarting Ransomware's New Playbook
- New AI Safety Initiative Aims to Set Responsible Standards for Artificial Intelligence
- New Class of CI/CD Attacks Could Have Led to PyTorch Supply Chain Compromise
- NSA Issues Guidance on Incorporating SBOMs to Improve Cybersecurity

Seen anything that you think should be on this list for our next edition? Let us know!

CPI Students <cpi.students@uwaterloo.ca>

Student Spotlights

DProvDB: Differentially Private Query Processing with Multi-Analyst Provenance

Shufan Zhang and Xi He
University of Waterloo

Our first student spotlight of 2024 comes to us from Shufan Zhang/CS, with their work entitled: DProvDB: Differentially Private Query Processing with Multi-Analyst Provenance.

Recent years have witnessed the adoption of differential privacy (DP) in practical database systems like PINQ, FLEX, and PrivateSQL. Such systems allow data analysts to query sensitive data while providing a rigorous and provable privacy guarantee. However, the existing design of these systems does not distinguish data analysts of different privilege levels or trust levels. This design can have an unfair apportion of the privacy budget among the data analyst if treating them as a single entity or waste the privacy budget if considering them as non-colluding parties and answering their queries independently. In this paper, they propose DProvDB, a fine-grained privacy provenance framework for the multi-analyst scenario that tracks the privacy loss to each single data analyst. Under this framework, when given a fixed privacy budget, they build algorithms that maximize the number of queries that could be answered accurately and apportion the privacy budget according to the privilege levels of the data analysts.

Find Out More about Digital Overground

Our mailing address is:

200 University Ave W. DC 3147 Waterloo, Ontario N2L 3G1