Digital Overground

Cybersecurity and Privacy Institute Student Newsletter

As the summer draws to a close, we hope that you had a fun break, or at the very least a productive season! Many of us don't get the summer off like we perhaps once did, so for those of you who continue to work or study in the summer months, we commiserate! Nonetheless, Fall is upon us, with a new school year beginning for a lot of folx. We wish everyone the very best in their studies, whether they are first year students about to begin the next exciting chapter of their lives, or the grizzled veterans who having been doing graduate work for years!

Please take the time to remember that we are all part of a larger community at Waterloo, regardless of where we are at in our work, we can always benefit by helping others and knowing when to take a break! Take care of yourselves and each other; may this coming year be as fun as it is enriching.

If you are interested in contributing to this newsletter, please email us at CPI Students <cpi.students@uwaterloo.ca> we welcome the help!

Upcoming Events

Uptown Waterloo Night Market

Night Swim Foam Bash

Mutts on Main

The Gaslight District Monster Market

[Open Air Antique Fair](#)

[In the Penal Colony: Performance and Symposium](#)

[Centre for Peace Advancement 10th Anniversary](#)

[Gidinawendamin/Ska'nikú•lát 21st Annual Pow Wow](#)

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

[Cyber Security Challenges within the Connected Home Ecosystem Futures](#)
Abdullahi Arabo

[Using Clustering Algorithms to Automatically](#)
[Identify Phishing Campaigns](#)
Kholoud Althobaiti, Maria K. Wolters, Nawal Alsufyani, & CPI Member Kami Vaniea

[AI and the Accounting Profession: Views from Industry and Academia](#)

CPI Members J. Efrim Boritz & Theophanis C. Stratopoulos

[Reducing the CNOT count for Clifford+T circuits on NISQ architectures](#)

Vlad Gheorghiu, Jiaxin Huang, Sarah Meng Li,

CPI Member Michele Mosca, & Priyanka Mukhopadhyay

[Phishing Codebook: A Structured Framework for the Characterization of Phishing Emails](#)

Tarini Saka, Rachiyta Jain, CPI Member Kami Vaniea, & Nadin Kökciyan

[What Do Mobile App Users Complain About?](#)

Hammad Khalid, Emad Shihab,

CPI Member Meiyappan Nagappan, &Ahmed E. Hassan

[Not as easy as just update: Survey of System Administrators and Patching Behaviours](#)

Adam Jenkins

Linsen Liu, Maria Wolters, & CPI Member Kami Vaniea

Open Calls

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

[ICITST 2024 : International Conference for Internet Technology and Secured Transactions](#)

[New York Annual Conference on Cyber Security 2024](#)
[December 14-15, 2024,](#)
[New York City](#)

[International Journal on Cybernetics & Informatics (IJCI)](#)

[WatITis 2024 Conference](#)

In the Media

- **Podcast of the Month: [Cybersecurity Today — In today's episode of Cyber Security Today, host Jim Love discusses a series of alarming cyber security incidents. Topics include a sophisticated attack exploiting a zero-day vulnerability in a popular network management platform, critical patches from SonicWall and Google addressing severe vulnerabilities, and an update on the National Public Data hack revealing deeper security issues. Learn about the latest threats and essential security measures you need to take now.](#)**
- **[How I found time for everything with a fulltime job](#)**
- **[Flipper Zero: Hottest Hacking Device?](#)**

- [**7 Free AI Productivity Tools I Use Every Day**](#)
- [**The European Union's World-First Artificial Intelligence Rules Are Officially Taking Effect**](#)
- [**Unlocking the Power of AI in Cybersecurity**](#)
- [**AI in the Enterprise: Cutting Through the Hype and Assessing Real Risks**](#)
- [**Ransomware Attacks on Industrial Firms Surged in Q2 2024**](#)
- [**Google Cloud Unveils New Security Services and Capabilities**](#)
- [**When Convenience Costs: CISOs Struggle with SaaS Security Oversight**](#)

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

[CPI Students <cpi.students@uwaterloo.ca>](mailto:cpi.students@uwaterloo.ca)

Cache Me If You Can: Accuracy-Aware Inference Engine for DP Data Exploration

Miti Mazmudar, Thomas Humphries, Jiaxiang Liu, Matthew Rafuse, and Xi He

Our August student spotlight is from Thomas Humphries/CS   Supervisor: Florian Kerschbaum with their poster: **Cache Me If You Can: Accuracy-Aware Inference Engine for Differentially Private Data Exploration**.

Differential privacy (DP) allows data analysts to query databases that contain users' sensitive information while providing a quantifiable privacy guarantee to users. Recent interactive DP systems such as APEx provide accuracy guarantees over the query responses but fail to support a large number of queries with a limited total privacy budget, as they process incoming queries independently from past queries. The team presents an interactive, accuracy-aware DP query engine, CacheDP, which utilizes a differentially private cache of past responses, to answer the current workload at a lower privacy budget, while meeting strict accuracy guarantees. They integrate complex DP mechanisms with their structured cache, through novel cache-aware DP cost optimization. Their thorough evaluation illustrates that CacheDP can accurately answer various workload sequences, while lowering the privacy loss as compared to related work.

Find Out More about Digital Overground

Our mailing address is:

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