CYBERSECURITY AND PRIVACY INSTITUTE
UNIVERSITY OF WATERLOO

Digital OverGround

Cybersecurity and Privacy Institute Student Newsletter

That picture is the most glorious and confounding thing you are likely to see today; laptop at the south pole, penguins are apparently fine with it, fair enough. The internet is a wonderful place sometimes, isn't it?

As the year draws to a close, we want to wish everyone the very best of luck with the end of their semester, we also hope that whatever you may be celebrating or doing over the winter break, that you stay safe and enjoy yourselves.

May the coming year bring us all more peace and greater knowledge.

Upcoming Events

Winterfest: 36th Annual Celebration

The Great Lakes and St. Lawrence Cities Initiative

Keeping Connected: An Evening of Indigenous Storytelling

Velocity call for Campus Ambassadors: Winter 2025

Winter Ice and Lights

Scran & Dram Scottish Public House

Gift of Lights

Ghosts of Christmas Past

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

Cyberheroes: The Design and Evaluation of an Interactive Ebook to Educate Children about Online Privacy

CPI Member Leah Zhang-Kennedy, Yomna Abdelaziz, & Sonia Chiasson

IRS: An Incentive-compatible Reward Scheme for Algorand

Maizi Liao, Wojciech Golab, & CPI Member Seyed Majid Zahedi

Productive play: The shift from responsible consumption to responsible production

CPI Member Jennifer Whitson & Martin French

PhishCoder: Efficient Extraction of Contextual Information from Phishing Emails

Tarini Saka, CPI Member Kami Vaniea, & Nadin Kökciyan

Local Community Care-based Activism and Civic Engagement Among Canadian Arab Youth

Melissa Finn & CPI Member Bessma Momani

ORTOA: A Family of One Round Trip Protocols For Operation-Type Obliviousness

CPI Member Sujaya Maiyya, Yuval Steinhart, Adrian Davila, Jason Du, Divyakant Agrawal, Prabhanjan Ananth, & Amr El Abbadi

Kamino: Constraint-Aware Differentially Private Data Synthesis

Chang Ge, Shubhankar Mohapatra, CPI Member Xi He, & Ihab F. Ilyas

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: SEC Cyber Disclosure Rules, Deloitte Hack Denial, and Critical Microsoft & SAP Patches - In this episode of Cybersecurity Today, host Jim Love delves into the ongoing confusion and compliance struggles faced by companies one year after the SEC's cyber disclosure rules were introduced. We analyze a BreachRx report revealing that less than 17% of public companies provide specific details in their cyber incident filings.**
- **Master Midjourney - Updated Beginner to Advanced Course**
- **YOU'RE VISUALIZING YOUR DATA WRONG. And Here's Why...**
- **AI generates accurate images of streets by listening to their soundtrack**
- **Microsoft, DOJ Dismantle Domains Used by Russian FSB-Linked Hacking Group**

- **GitHub Launches Fund to Improve Open Source Project Security**
- **The Ghost of Christmas Past – AI's Past, Present and Future**
- **Cybercriminals Are Increasingly Helping Russia and China Target the US and Allies, Microsoft Says**
- **Phishing: The Silent Precursor to Data Breaches**
- **Now on Demand: Inside a Hacker's Playbook – How Cybercriminals Use Deepfakes**

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

Our December Student Spotlight features the CPI Poster competition 3rd place winners, **Yuzhe You and Jarvis Tse** Supervisor: Jian Zhao CS, with their work entitled: **AdvEx: Understanding Adversarial Attacks with Interactive Visualizations**

Adversarial machine learning (AML) focuses on studying attacks that can fool machine learning algorithms into generating incorrect outcomes as well as the defenses against worst-case attacks to strengthen the adversarial robustness of machine learning models. Specifically for image classification tasks, it is difficult to comprehend the underlying logic behind adversarial attacks due to two key challenges: 1) the attacks exploiting “non-robust” features that are not human-interpretable and 2) the perturbations applied being almost imperceptible to human eyes. They propose an interactive visualization system, AdvEx, that presents the properties and consequences of evasion attacks as well as provides data and model performance analytics on both instance and population levels. They quantitatively and qualitatively assessed AdvEx in a two-part evaluation including user studies and expert interviews. Their results show that AdvEx is effective both as an educational tool for understanding AML mechanisms and a visual analytics tool for inspecting machine learning models, which can benefit both AML learners and experienced practitioners.

Find Out More about Digital Overground

Our mailing address is:

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