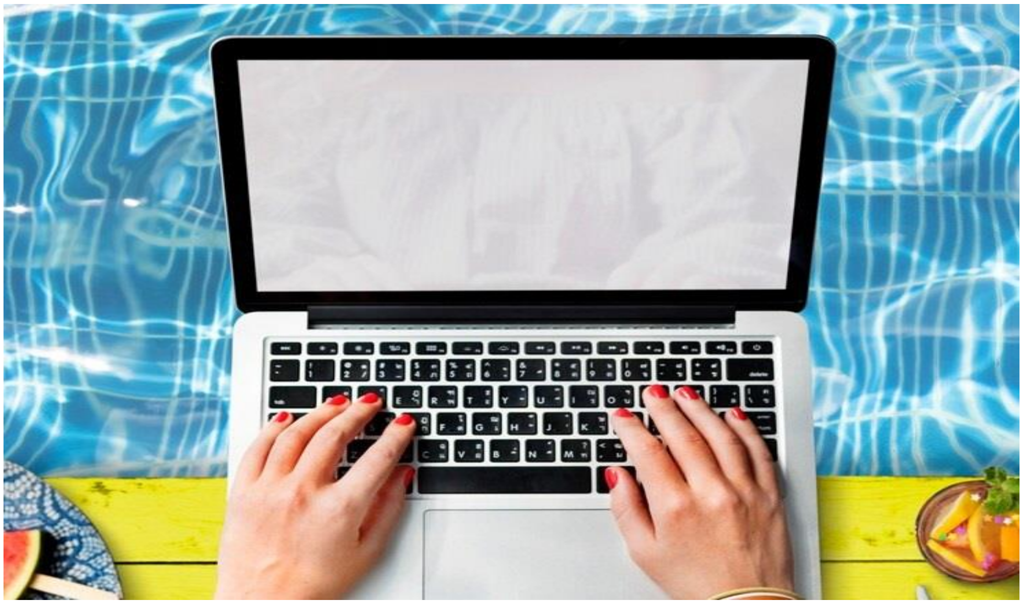
CYBERSECURITY
AND PRIVACY INSTITUTE
UNIVERSITY OF WATERLOO

Digital Overground

Cybersecurity and Privacy Institute Student Newsletter



We are hoping you “May” enjoy this spring edition of Digital OverGround, hence the dad pun to start things off! We all need a vacation, so let’s just let it slide 😉

Keeping in mind that for many folx the summer semester means just as much schoolwork or regular-get-paid-money work, we still hope that at some point you get to do something similar to the picture above, where one may be working but at least you are outdoors while doing it!

Regardless, *may* this be the start of a good summer for us all.

(we know, that’s two puns, we promise we will work on it)

As always, we strongly nudge you towards contributing to this newsletter, so please email us at CPI Students <cpi.students@uwaterloo.ca> we welcome the help!

Upcoming Events

Open Ears | Festival of Music & Sound

WISE Public Lecture

Formlabs | Fall Co-ops IN-PERSON Information Session

Velocity Pitch Competition (Application Deadline)

Pride Month 2024 Flag Raising Ceremony

Future-ready workforce series:
Building inclusive workplaces for 2SLGBTQIA+ students

Engineering Graduate Studies Fair

CPI Talk - Characterizing Machine Unlearning through Definitions and Implementations

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

Choosing Public Datasets for Private Machine Learning via Gradient Subspace Distance

Xin Gu, CPI Member Gautam Kamath, & Zhiwei Steven Wu

Side-Channel Attacks on Optane Persistent Memory

CPI Member Sihang Liu, Suraaj Kanniwadi, Martin Schwarzl, Andreas Kogler, Daniel Gruss, & Samira Khan

Profiling Hyperscale Big Data Processing

Abraham Gonzalez, Aasheesh Kolli, Samira Khan, CPI Member Sihang Liu, Vidushi Dadu, Sagar Karandikar, Jichuan Chang, Krste Asanović, & Parthasarathy Ranganathan

Speaking Out against Socially Destructive Technologies

Katina Michael, CPI Member Heather A. Love, & Judy Wajcman

Implicit Stylization for Domain Adaptation

Jinman Park, Francois Barnard, Saad Hossain, & CPI Member Sirisha Rambhatla

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)

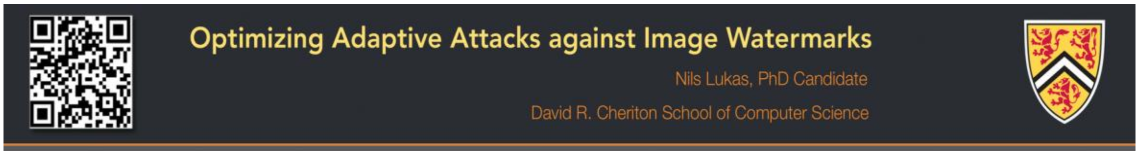
In the Media

- **Podcast of the Month:** Cybersecurity Today – A New North Korean ransomware gang spotted, This episode reports on ransomware news, US sanctions against Chinese citizens for running a botnet, and more
- CPI hosted the 2024 CyberTitan National Finals
- How I'd Learn AI (If I Had to Start Over)
- You need to learn AI in 2024! (And here is your roadmap)
- 23 AI Tools You Won't Believe are Free
- Zoom Adding Post-Quantum End-to-End Encryption to Products
- User Outcry as Slack Scrapes Customer Data for AI Model Training
- EPA Issues Alert After Finding Critical Vulnerabilities in Drinking Water Systems
- Critical Vulnerability in Honeywell Virtual Controller Allows Remote Code Execution
- Google Cites 'Monoculture' Risks in Response to CSRB Report on Microsoft

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



Optimizing Adaptive Attacks against Image Watermarks

Nils Lukas, PhD Candidate

David R. Cheriton School of Computer Science

Our May student spotlight is from Nils Lukas/CS (Supervisor: Florian Kerschbaum) with his poster: **Leveraging Optimization for Adaptive Attacks against Image Watermarks** .

Untrustworthy users can misuse image generators to synthesize high-quality deepfakes and engage in online spam or disinformation campaigns. Watermarking deters misuse by marking generated content with a hidden message, enabling its detection using a secret watermarking key. A core security property of watermarking is robustness, which states that an attacker can only evade detection by substantially degrading image quality. Assessing robustness requires designing an adaptive attack for the specific watermarking algorithm. A challenge when evaluating watermarking algorithms and their (adaptive) attacks is to determine whether an adaptive attack is optimal, i.e., it is the best possible attack. They solve this problem by defining an objective function and then approach adaptive attacks as an optimization problem. The core idea of their adaptive attacks is to replicate secret watermarking keys locally by creating surrogate keys that are differentiable and can be used to optimize the attack's parameters. They demonstrate for Stable Diffusion models that such an attacker can break all five surveyed watermarking methods at negligible degradation in image quality. These findings emphasize the need for more rigorous robustness testing against adaptive, learnable attackers.

Find Out More about Digital Overground

Our mailing address is:

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