CYBERSECURITY
AND PRIVACY INSTITUTE
UNIVERSITY OF WATERLOO

Digital Overground

Cybersecurity and Privacy Institute Student Newsletter

This is the April Edition, which means end of term!! And for some, graduation! For others, who are still banging away at their academic pursuits, this may not be a notable date as they are perhaps studying through the summer, with graduation still to come.

We would like to take a minute though, to express our thoughts for everyone who has studied at Waterloo. Whether you are graduating now (and congratulations!), or still have a ways to go, let's all take a beat and be thankful for the opportunities we have had here.

Education is a wonderful thing, and while it isn't perfect, and there isn't equal access to it for everyone, we can all take a moment to reflect on our journeys and what they mean to us, and those who we have shared them with.

We hope that whether you are sticking around for a bit longer, or you are off to your next chapter, that you continue to grow and learn regardless of where you are, that you share your knowledge with others and are always open to learning from them in return.

Whatever your goals in life, we hope you achieve them, and that you try to help others achieve theirs.
Have a wonderful summer!

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

Graduate House Upcoming Events

Spring Tree Planting

BioBlitz

Kalihwíyo Indigenous Art Market Pop Up

Behnaz Fatemi We will lose our beloveds

Hops & High Notes: Opera at the Brewery

Elmira Theatre Company presents The Drowning Girls

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

Streaming Quantum State Purification

Andrew M. Childs, Honghao Fu, CPI Member Debbie Leung,
Zhi Li, Maris Ozols, and Vedang Vyas

Conditional Disclosure of Secrets with Quantum Resources

Vahid R. Asadi, Kohdai Kuroiwa, CPI Member Debbie Leung, Alex May,
Sabrina Pasterski, and Chris Waddell

The Role of Adaptive Optimizers
for Honest Private Hyperparameter Selection

Shubhankar Mohapatra, CPI Member Sajin Sasy, CPI Member Xi He,
CPI Member Gautam Kamath, and Om Thakkar

MIDE: Accuracy Aware Minimally Invasive Data Exploration For Decision Support

Sameera Ghayyur, Dhrubajyoti Ghosh, CPI Member Xi He, and Sharad Mehrotra

The Aurora Single Level Store Operating System

Emil Tsalapatis, Ryan Hancock, Tavian Barnes,
and CPI Member Ali José Mashtizadeh

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

2024 American Society of Criminology Annual Meeting

The 2024 ASC Annual Meeting will be held at Marriott Marquis in San Francisco, CA from November 13-16, 2024. This year's theme is *Criminological Research and Education Matters: People, Policy, and Practice in Tumultuous Times*. Abstracts for thematic panels, individual papers, and author meets critic sessions are **due Friday, March 22, 2024.** Abstracts for posters, roundtable sessions and lightning talks are due **Friday, May 17, 2024.**

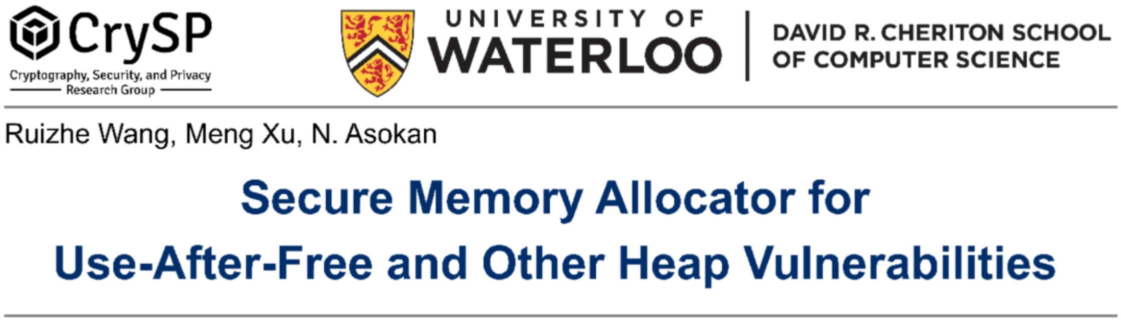
In the Media

- **Podcast of the Month:** Cybersecurity Today – This episode reports on the danger of using expired open-source packages, a tool used by a Russian hacking group and password advice
- I Analyzed My Finance with Local LLMs
- What are you going to do in 2024? Tops 5 skills to get!
- Generative AI in a Nutshell - how to survive and thrive in the age of AI
- What's the future for generative AI? - The Turing Lectures with Mike Wooldridge
- Chrome to Fight Cookie Theft with Device Bound Session Credentials
- Microsoft DRM Hack Could Allow Movie Downloads from Popular Streaming Services
- Number of Chinese Devices in US Networks Growing Despite Bans
- Inside AWS's Crusade Against IP Spoofing and DDoS Attacks

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


CrySP
Cryptography, Security, and Privacy Research Group
UNIVERSITY OF WATERLOO
DAVID R. CHERITON SCHOOL OF COMPUTER SCIENCE

Ruizhe Wang, Meng Xu, N. Asokan

Secure Memory Allocator for Use-After-Free and Other Heap Vulnerabilities

Our March student spotlight is from Ruizhe Wang/CS (Supervisor: N. Asokan & Meng Xu) with his poster: Secure Memory Allocator for Use-after-free and other Heap Vulnerabilities.

Attacks on heap memory, encompassing memory overflow, double and invalid free, use-after-free (UAF), and various heap spraying techniques are ever-increasing. Existing entropy-based secure memory allocators provide statistical defenses against virtually all of these attack vectors. Although they claim protections against UAF attacks, their designs are not tailored to detect (failed) attempts. Consequently, to beat this entropy-based protection, an attacker can simply launch the same attack repeatedly with the potential use of heap spraying to further improve their chance of success. They introduce a novel allocator, aiming to enhance UAF-attempt detection without compromising other security guarantees or introducing significant performance overhead. To achieve this, they use three innovative constructs in secure allocator design: free block canaries (FBC) to detect UAF attempts, random in-block offset (RIO) to stop the attacker from accurately overwriting the victim object, and random bag layout (RBL) to impede attackers from estimating the block size based on its address. They show that compared to state-of-the-art entropy-based allocators, it improves UAF-protection without incurring additional performance overhead. Compared to UAF-mitigating allocators, it trades off a minuscule probability of failed protection for significantly lower overhead.

Find Out More about Digital Overground

Our mailing address is:

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