He (Shawn) Shuang

Looking for full-time and internship opportunities for Summer/Fall 2025
+1 4168230889 8759shuang@gmail.com

SUMMARY

PhD candidate in Web Security and Computer Engineering at the University of Toronto, with a strong focus on improving security and privacy in web applications. Experienced in network security, system security, and software vulnerability analysis, with hands-on expertise in defending against user-impersonation attacks, detecting web trackers, and mitigating security risks in software-defined networks. Proven track record in academic research with multiple peer-reviewed publications in top-tier conferences such as NDSS and DSN. Proficient in programming languages such as Python, R, C/C++, and tools including fuzzers, dynamic analysis frameworks, and machine learning libraries. Currently seeking full-time research or software engineering roles for Summer/Fall 2025, with a strong desire to apply advanced security techniques in industry settings.

EDUCATION

Doctor of Philosophy (PhD), *University of Toronto* 2020 - 2025
Web Security, Computer Engineering Supervisor Prof. David Lie

- Thesis: Improving the security and privacy of client-generated requests in web applications
- Project #1: Defending against user-impersonation attacks with client-side request certification systems
- Project #2: Detecting web trackers (non-mixed and mixed) with a breakage detector
- Side projects: Program debloating through dynamic analysis, program fuzzing

Master of Applied Science (MASc), University of Toronto 2017 - 2020
Network Security, Computer Engineering Supervisor Prof. David Lie

- Project: defending against pervasive monitoring in software-defined networks (SDN)

Honours Bachelor of Science (HBSc), University of Toronto 2011 - 2016
Computer Science with a focus on Web and Internet High distinction, Dean's list (all years)

SELECTED PUBLICATIONS

- [NDSS 2025] He Shuang, Lianying Zhao, David Lie. 2025. "Duumviri: Detecting Trackers and Mixed Trackers with a Breakage Detector"
  - A framework for non-mixed and mixed tracker detector using a combination of tracking detector and breakage detector

- [CSUR 2024] Lianying Zhao, He Shuang, Shengjie Xu, Wei Huang, Rongzhen Cui, Pushkar Bettadpur, and David Lie. 2024. "A Survey of Hardware Improvements to Secure Program Execution"

- [DSN 2023] He Shuang, Lianying Zhao, David Lie. 2023. "vWitness: Certifying Web Page Interactions with Computer Vision". Acceptance rate 19.58%.
  - A novel framework for request certification for user-impersonating attacks under privileged malware

- [APSys 2019] He Shuang, Wei Huang, Pushkar Bettadpur, Lianying Zhao, Ivan Pustogarov, and David Lie. 2019. "Using Inputs and Context to Verify User Intentions in Internet Services"

    - A position paper that uses TEEs like Intel SGX and trusted hypervisors together to solve security issues
- [arXiv] Pushkar Bettadpur, He Shuang, David Lie. 2019. "TrafFu: An SDN-based Defense against Pervasive Monitoring"

EMPLOYMENT

Researcher, Huawei Waterloo Research Center 2024 - Current

- LLM-based Software Security Management Framework for early vulnerability identification
    - Implemented the first internal Software Security Management Framework (SSMF) that automatically produces vulnerability reports for software owner and users
    - Enhanced SSMF with RAGs to enhance report quality
    - Reduced internal vulnerability triage time on the software user side by a factor of three

Teaching Assistant, University of Toronto 2019 - 2024

- Paper summary grading, lab preparation, lab grading and answer student questions

Research Assistant, University of Toronto, with Prof. Harald Bathelt 2021 - 2024

- Economics data analysis and model building in R

Software Developer, Trapeze Group, Mississauga 2014-2015 (Intern), 2016-2017 (Full Time)

- Front (JavaScript in MVC architecture) and back end (C++, SQL) web-based application development

SKILLS

- *Web Security*: OWASP Top 10, crawling (Selenium), malicious script detection & anti-detection(ML-based)
- *Network Security*: OSI stack, bot detection and anti-detection, SDN network simulation (Mininet), traffic analysis & obfuscation (ML-based), network cache (Squid, MITMproxy), packet sniffers (Wireshark)
- *System Security*: vulnerability analysis (fuzzing), malware identification (ML-based), attack surface reduction (dynamic and static program analysis), trusted IO (under privileged attacker), reverse engineering (Frida), program control flow and data flow analysis (LLVM-based)
- *Programming Languages*: Python (model building), R (statistical analysis), SQL, Javascript, C/C++
- *Machine Learning Libraries*: Numpy, Scikit-learn, TensorFlow, Keras, PyTorch

AWARDS

- Bell Scholarship, University of Toronto 2020 - 2023
- Ontario Graduate Scholarship, University of Toronto 2017 - 2020
- In-course Scholarship, University of Toronto 2012

COMMUNITY SERVICE

- Volunteer, ACM SOSP 2019
- Volunteer, ACM CCS 2018