THE CHINESE UNIVERSITY OF HONG KONG

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING &
DEPARTMENT OF INFORMATION ENGINEERING
JOINT SEMINAR

AI-DRIVEN FUZZING ACROSS THE SOFTWARE STACK

Abstract:

Fuzzing is a popular technique for finding software defects automatically. However, it is challenging to fuzz efficiently at different levels of the software stack. I will share our work on applying AI techniques to fuzzing applications, libraries, and LLVM IR. For applications, we transform a program into a multivariate function over its input values, formulate fuzzing as an optimization problem, and apply machine learning algorithms to the optimization problem. For libraries, we use a Large Language Model to iteratively generate fuzz drivers, and use code coverage to guide the fuzzer to explore undiscovered library code. For LLVM IR, we guarantee input validity while increasing input diversity using constrained mutations and collect accurate coverage feedback by tracking the matcher table. I will discuss the power of AI in fuzzing, the challenges, and future directions.

Biography:

Ho Chen is a chair professor at the University of Hong Kong. His current research interests are AI-driven security and software engineering, and AI security and robustness. He is a fellow of IEEE. More information is available at https://sec.hku.hk

27 NOV 2024 (WED)
2:30pm - 3:30pm

SHB801, 8/F, Ho Sin Hang Engineering Building (SHB)

Professor CHEN Ho

Chair Professor
Institute of Data Science &
Department of Computer Science
The University of Hong Kong

Enquiries:

- Professor MENG Wei (wei@cse.cuhk.edu.hk)
- Professor Wing C. LAU (wclau@ie.cuhk.edu.hk)
- Mr. WONG O Bong (obong@cse.cuhk.edu.hk)
- Ms. Vivien Ng (vivien@cse.cuhk.edu.hk)