In Favour of Posting

THE CHINESE UNIVERSITY OF HONG KONG

Department of Information Engineering

Seminar

Automated Analysis for Memory Corruption Vulnerabilities: From Classification, Assessment to Exploitation

by

Prof. Feng Chao

National University of Defense Technology , China

Date : 29 Aug 2025 (Friday)

Time : 2:00pm – 3:00pm

Venue : Rm 801, Ho Sin-hang Engineering Building, CUHK

Abstract

Memory corruption vulnerabilities remain among the most critical threats in cybersecurity. Analyzing the vast number of crash samples generated by fuzzing or other techniques poses a significant challenge. Our research aims to develop automated and intelligent solutions to streamline this process, from initial triage to full exploit verification.

This presentation will introduce a series of automated vulnerability analysis systems developed by our research team, addressing three critical stages of the vulnerability analysis pipeline:

1. Automated Crash Classification: We have developed an efficient system for automatically categorizing a large volume of crash samples based on their root causes. This work significantly accelerates the initial triage process, allowing analysts to quickly identify and prioritize unique and high-severity vulnerabilities from massive datasets.
2. Automated Exploitability Assessment: To move beyond simple crash replication, our team has created a novel framework for dynamically assessing the true severity and exploit potential of a vulnerability. This technique analyzes the program state at the time of crash to automatically determine the possible attacker capabilities (e.g., arbitrary read/write), providing critical data for risk assessment.
3. Automated Exploit Generation: We have designed a method to automatically generate inputs that manipulate memory layouts to construct reliable proof-of-concept exploits. Given a initial PoC that triggers a crash, this technology solves the key challenge of reliably crafting necessary memory structures (e.g., heap states) to demonstrate full exploitability, turning a theoretical vulnerability into a practical security threat.

Biography

Feng Chao is an Associate Professor and Director of the Cognitive Communications Department at the College of Electronic Science and Technology, National University of Defense Technology (NUDT). He received his B.S., M.S., and Ph.D. degrees in Information & Communication Engineering from NUDT.

Professor Feng's research focuses on automated software vulnerability analysis and wireless network security. He leads a group that has discovered over 80 vulnerabilities in operating systems, office software, and embedded devices. He has presided over more than 10 key projects, including topics under the National Key R&D Program of China. He has been awarded three Ministerial and Provincial-Level Science and Technology Progress Awards (Second Prize).

He founded the halfbit cybersecurity team, which under his guidance won multiple championships in the Robot Hacking Game for automated vulnerability analysis and received the AI Innovation Award at Defcon China. Professor Feng has published more than 20 papers in peer-reviewed journals and conferences, including multiple publications in top-tier security conferences such as NDSS, USENIX Security, and CCS, as well as in leading domestic journals.

**** ALL ARE WELCOME ****

Host: Prof. ZHANG Kehuan (Tel: 3943-8391, Email: kehuan@ie.cuhk.edu.hk)
Enquiries: Information Engineering Dept., CUHK (Tel.: 3943-8467)