DISTINGUISHED LECTURE SERIES

Scaling Formal Verification for Real System Software

Prof. Jason Nieh

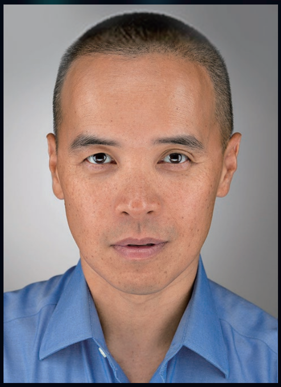
Computer Science, Columbia University (USA)

Monday, June 23, 2025 10:00am
Auditorium106 at IIS new Building

Abstract

System software is widely used yet increasingly complex, making it difficult to eliminate vulnerabilities that pose significant security risks. Formal verification offers a possible solution, but remains impractical for verifying unmodified, real-world system software. To address this problem, I will present Spoq, a highly automated verification framework that leverages Coq and Z3 to scale formal verification for real-world system software with much less proof effort. Instead of manually writing specifications, which is error-prone, Spoq uses a set of verified rules to automatically generate high-level specifications from unmodified software implementations that can be used to prove higher-level properties such as security. I will discuss some recent verification results using Spoq, including verifying, for the first time, the unmodified open-source firmware for the Arm Confidential Compute Architecture.

Biography



Jason Nieh is Professor of Computer Science and Co-Director of the Software Systems Laboratory at Columbia University. Technologies he developed are widely used in major operating system platforms, including Android and Linux, the largest cloud infrastructure providers, including Amazon Web Services and Google Cloud, and ubiquitous Arm processors, billions of which ship each year. Nieh is a Fellow of the AAAS, ACM, IEEE, and John Simon Guggenheim Memorial Foundation. Other honors for his research work include a Sigma Xi Young Investigator Award, a National Science Foundation CAREER Award, a Department of Energy Early Career Award, numerous industry research awards, including those from Amazon, Google, and IBM, and various best paper and test of time awards, including those from MobiCom, OSDI, SIGCSE, SIGMETRICS, and SOSP. A dedicated teacher, he received the Distinguished Faculty Teaching Award for his innovations in teaching operating systems and for introducing virtualization as a pedagogical tool, which has become common practice at universities around the world. Nieh earned his B.S. from MIT and his M.S. and Ph.D. from Stanford University, all in Electrical Engineering.

中央研究院 資訊科學研究所
Institute of Information Science, Academia Sinica

For more information:
http://www.iis.sinica.edu.tw/