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

Distinguished Lecture Series

# Design and Verification of the Arm Confidential Compute Architecture

**Tuesday, Jun. 27, 2023 10:00am**
**Auditorium 106, at IIS new Building**


## Prof. Jason Nieh

Computer Science, Columbia University (USA)



## Abstract

The increasing use of sensitive private data in computing is matched by a growing concern regarding data privacy. System software such as hypervisors and operating systems are supposed to protect and isolate applications and their private data, but their large codebases contain many vulnerabilities that can risk data confidentiality and integrity. I will discuss our work on Realms, a new abstraction for confidential computing to protect the data confidentiality and integrity of virtual machines. Hardware creates and enforces Realm world, a new physical address space for Realms. Firmware controls the hardware to secure Realms and handles requests from untrusted system software to manage Realms, including creating and running them. Untrusted system software retains control of the dynamic allocation of memory to Realms, but cannot access Realm memory contents, even if run at a higher privileged level. To guarantee the security of Realms, we verified the firmware, introducing novel verification techniques that enable us to prove, for the first time, the security and correctness of concurrent software with fine-grained locking and dynamically allocated shared page tables, data races in kernel code running on relaxed memory hardware, integrated C and Arm assembly code calling one another, and untrusted software being in full control of allocating system resources. Realms are included in the Arm Confidential Compute Architecture and Armv9, the next version of the Arm CPU architecture.


## Biography

Jason Nieh is Professor of Computer Science at Columbia University. Technologies he developed are widely used in major operating system platforms, including Android and Linux, and are built into Arm processors, billions of which ship each year. He was the first to use virtualization as a classroom teaching tool, which has become common practice at universities around the world. Nieh is a Fellow of the 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 awards, including those from MobiCom, OSDI, SIGCSE, SIGMETRICS, and SOSP. Nieh earned his B.S. from MIT and his M.S. and Ph.D. from Stanford University, all in Electrical Engineering.

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