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

Distinguished Lecture Series

Towards Trustworthy Systems

Thursday, October 13th, 2011 10:00am
Auditorium 106 at New IIS Building

Gernot Heiser

Scientia Professor and John Lions Chair of Operating Systems,
School of Computer Science and Engineering,
The University of New South Wales Sydney

Abstract

Computer systems are routinely deployed in life- and mission- critical situations, yet in most cases their security, safety or dependability cannot be assured to the degree warranted by the application. In other words, trusted computer systems are rarely trustworthy.

We believe that this is highly unsatisfactory, and have embarked on a research program aimed at bringing reality in line with expectations. In this talk describes NICTA's research agenda for achieving true trustworthiness in systems. The approach is based on establishing the trustworthiness of the lowest level of software, a small microkernel or hypervisor, and then using this platform to provide guarantees to complete systems built on top. A number of important steps in this direction have been achieved, specifically the formal proof of functional correctness of a complete OS microkernel, and subsequently the establishment of further properties, including timeliness and integrity enforcement. Work is progressing on making dependability guarantees for complete real-world systems, comprising millions of lines of code.

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