THE UNIVERSITY OF
CHICAGO
Computer Science Department

CERES UNSTOPPABLE SPEAKER SERIES

Frans Kaashoek

Professor

Massachusetts Institute of Technology

December 6, 2018, Crerar 298 at 4:00pm

"Verifying a file system: correctness in presence of crashes"

Abstract:
As a case study of system software verification, this talk will describe FSCQ, the first file system with a machine-checkable proof (using the Coq proof assistant) that its implementation meets its specification and whose specification includes crashes. FSCQ provably avoids bugs that have plagued previous file systems, such as performing disk writes without sufficient barriers or forgetting to zero out directory blocks. If a crash happens at an inopportune time, these bugs can lead to data loss. FSCQ's theorems prove that, under any sequence of crashes followed by reboots, FSCQ will recover the file system correctly without losing data. This talks describes how we wrote FSCQ's specification and how we proved that FSCQ's implementation meets its specification. Although FSCQ is a simple file system, our experience with FSCQ suggests that formal verification is ready for certifying system software, opening up many interesting and challenging research problems. Joint work with: Tej Chajed, Haogang Chen, Atalay İleri, Adam Chlipala, Nickolai Zeldovich.

Bio:
Frans Kaashoek is the Charles Piper Professor in MIT's EECS department and a member of CSAIL, where he coleads the parallel and distributed operating systems (PDOS) group. He received his PhD from the Vrije Universiteit (Amsterdam, The Netherlands) for his work on group communication in the Amoeba distributed operating system. Frans is a member of the National Academy of Engineering and the American Academy of Arts and Sciences, the recipient of the ACM SIGOPS Mark Weiser award and the 2010 ACM Prize in Computing. He was a cofounder of Sightpath, Inc. and Mazu Networks, Inc.

CERES
Center for Unstoppable Computing

The talk is at 4:00pm, Thursday, December 6, Crerar 298

Refreshments during talk, Crerar 298

Host: Haryadi Gunawi
Contact: 773-702-3508
http://www.cs.uchicago.edu/events