The 8th IEEE International Conference on Software Security and Reliability

SERE 2014

San Francisco, CA, USA, June 30-July 2, 2014

http://paris.utdallas.edu/sere14

Keynote Speech

Software Fault Tolerance

Kishor Trivedi
Fitzgerald S. Hudson Professor
Department of Electrical and Computer Engineering
Duke University
www.ee.duke.edu/~ktrivedi

Abstract

The size of software present in safety critical and other technical systems has been growing by leaps and bounds. Several recent studies have established that most system outages are due to software faults. Traditional methods of fault avoidance, fault removal based on extensive testing/debugging, and fault tolerance based on design/data diversity are found wanting due to the increasing complexity of software. The key challenge then is how to provide highly dependable software in complex software-based environments. We discuss a new view of fault tolerance of software systems. We classify software faults into Bohrbugs and Mandelbugs, and identify aging-related bugs as a subtype of the latter. Traditional methods have been designed to deal with Bohrbugs. The next challenge then is to develop mitigation methods for Mandelbugs in general and aging-related bugs in particular. We submit that mitigation methods for Mandelbugs utilize environmental diversity. Retry operation, restart application, failover to an identical replica (hot, warm or cold) and reboot the OS are examples of mitigation techniques that rely on environmental diversity. For software aging related bugs it is also possible to utilize proactive environmental diversity technique known as software rejuvenation. We discuss environmental diversity both from experimental and analytic points of view and cite examples of real systems employing these techniques.

About the speaker

Kishor S. Trivedi holds the Hudson Chair in the Department of Electrical and Computer Engineering at Duke University, Durham, NC. He has been on the Duke faculty since 1975. He is the author of a well known text entitled, Probability and Statistics with Reliability, Queuing and Computer Science Applications, published by John Wiley. He is a Fellow of the Institute of Electrical and Electronics Engineers. He has published over 500 articles and has supervised 45 Ph.D. dissertations. He is the recipient of IEEE Computer Society Technical Achievement Award

for his research on Software Aging and Rejuvenation. He works closely with industry in carrying our reliability/availability analysis, providing short courses on reliability, availability, and in the development and dissemination of software packages such as SHARPE, SREPT and SPNP. His algorithm was used in the reliability analysis of the current return network subsystem of Boeing 787 for the purpose of FAA certification. Reliability/availability analysis of SIP on Websphere he conducted for IBM was responsible for the sale of the system to a Telco customer. He helped implement software rejuvenation in IBM x-series. Currently he is focused on the study of software faults, failures caused by these faults and the mitigations techniques to deal with the failures.