Simple Techniques for Eliminating Fatal Errors in Software Systems
April 24, 2009

Speaker: Dr. Martin Rinard
Department of Electrical Engineering and Computer Science
Computer Science and Artificial Intelligence Laboratory
Massachusetts Institute of Technology

Abstract

I will present a set of simple techniques that enable software systems to survive otherwise fatal errors. The goal is to enable systems to execute through such errors, potentially with degraded functionality, to continue to serve the needs of their users.

For each class of fatal error I present a simple technique that eliminates the error and enables the program to continue to execute. For example, the technique that eliminates out of bounds array accesses simply discards out of bounds writes and manufactures values for out of bounds reads.

While these techniques are straightforward to implement and deploy, they perturb the standard programming language semantics and introduce the possibility of taking the system down unanticipated execution paths. As such, they represent a significant departure from standard approaches. I will discuss the benefits and risks of adopting such techniques and present experimental results that illustrate the potential implications of using the techniques in large software systems.

Dr. Martin Rinard