

Survivability Analysis of Networked Systems

Jeannette M. Wing
Carnegie Mellon University

Survivability is the ability of a system to continue operating despite the presence of abnormal events such as failures and intrusions. Ensuring system survivability has increased in importance as critical infrastructures have become heavily dependent on computers. In this talk I will present a systematic method for performing survivability analysis of networked systems. An architect injects failure and intrusion events into a system model and then visualizes the effects of the injected events in the form of scenario graphs. Our method enables further global analyses, such as reliability, latency, and cost-benefit analyses, where mathematical techniques used in different domains are combined in a systematic manner. In particular, we draw on symbolic model checking, constrained Markov Decision Processes, and Bayesian networks to affect our method. I will illustrate the method on an abstract model of the United States Payment System. This work is done jointly with Somesh Jha.