

David A. Fisher
Software Engineering Institute
412-268-7703
dfisher@cert.org

I conduct research on various aspects of survivability in unbounded systems at CERT/CC. A fundamental assumption in my work is that it is impossible to prevent compromises of any particular component of a system or network. Thus, survivability is the ability of a system to continue to satisfy its critical mission requirements in the presence of attacks, accidents and failures (of system components). Central to our approach is emergent algorithms. Emergent algorithms generate and maintain specified system wide properties that characterize the mission requirements, they must be flexible and adaptive, and to be cost-effective they must consume less than order n^2 resources where n is the number of nodes in the system. To gain understanding of survivability, unbounded systems and emergent algorithms, to validate and test our models, theories and solutions, and to demonstrate findings we have developed a property-based modeling and simulation language called Easel. Easel is most appropriate for specifying accurate abstract models of anything. It allows separate specification of simulations that incorporate the models. Simulations may include any desired instrumentation and multiple views with dynamic graphic depictions. Recent work has focused on emergent algorithms for IP routing and enhancements for survivability for fixed, mobile and ad hoc networks. Proposed discussion topics are: (1) How crucial is trust to survivable systems and how can it be maintained? (2) Can simulation and/or analysis be effective in validating survivable solutions, and what are the alternatives?