Axiomatic Analysis and Cyber Threat Tree Models for the Development of Large-Scale Disaster-Tolerant Information Security Systems

Theodore W. Manikas and Mitchell A. Thornton
Dept. of Computer Science and Engineering
Southern Methodist University
(manikas@lyle.smu.edu, mitch@lyle.smu.edu)

Disaster tolerance in computing and communications systems refers to the ability to maintain a degree of functionality throughout the occurrence of a disaster. We accomplish the incorporation of disaster tolerance within a system by simulating various threats to the system operation and identifying areas for system redesign. Such areas are then analyzed and redundancy is added to enhance tolerance. Unfortunately, many systems are too large to be simulated in a time effective manner.

A method for decomposing the system into smaller, more computationally practical subsystems is developed to alleviate this difficulty. The ability to simulate subsystems of the larger system and then combine the results to achieve overall system simulation response enables disaster tolerance methods to be assessed for the system as a whole before they are deployed. Therefore, we apply a method that we devised called axiomatic analysis to solve this problem.

The axiomatic analysis approach decomposes an existing large system into subsystems, based on axioms similar to those used in axiomatic design. Each subsystem is then small enough to be simulated in a time effective manner so that analysis can be performed and redundancy can be included only where needed. The axiom of subsystem independence will allow unanticipated subsystem interdependencies that occurred due to the evolution of the overall system topology to be uncovered. Once the interdependencies are uncovered, intelligent decomposition can occur and points where redundancy should be added to enhance disaster tolerance can be identified. Furthermore, the independence axiom allows the "divide and conquer" approach to simulation to be successful since the relatively independent subsystems obey the principle of superposition when the overall response is synthesized.

In the ultimate goal of enhancing existing large systems to add resiliency in the presence of a disaster, it is necessary to catalog identified threats and determine the importance of each threat. This analysis could enable redundancy to be added at key points in the system to provide some degree of disaster tolerance. A simple list of all possible threats is not amenable to this type of analysis particularly when the list of threats is large and contains many common sub-elements. Furthermore, it can be difficult to rank the priority of the individual threats when they are described as a list with a corresponding disaster event attached to each. To overcome these difficulties, we have developed and use the concept of cyber threat trees which are a generalization of the fault or threat tree ideas previously used for classical system fault tolerance and analysis.

Cyber Threat Trees are a superset of fault and attack trees since they are based on multiple-valued or radix-p valued algebras over a finite and discrete set of values. When the radix p=2, the cyber threat tree reduces to a fault or attack tree depending on the nature of the disruptive events. Generally, cyber threat trees have p>2: these additional logic states allow for more complicated interactions to be modeled. The advantage of cyber threat trees is that they are very compact representations of a large number of threats, they automatically illustrate threat commonalities, and due to their canonical structure, they are suitable for implementation of automatic analysis algorithms.