

Survivability Modeling and Analysis

by Seungchan Oh

Our dependence on Information Technologies (IT) has introduced a new form of vulnerability that gives cyber-attackers the opportunity to launch attacks against our national infrastructure (national defense systems, air traffic control systems, power grid control systems, etc.) . Understanding the vulnerability of our Cyber-infrastructure and how to quantify it becomes critically important to secure and protect our IT services and resources. The formal definition of survivability is the ability of the system to provide essential services in case of faults, attacks or accidents in a timely manner. Security in general focuses on recognition and resistance of attacks, but survivability includes faults and accidents.

The quantification of survivability can be used to analyze the robustness and survivability of different topologies and distribution of cyberspace resources. Additionally we can improve the survivability of a system by locating the vulnerable hardware and/or software components so they can be hardened. Very few research has been conducted to quantify the survivability of IT systems and their services due to its challenging complexity. In our approach, we adopt Ellison's description of survival systems that should have three properties (3R) – Resistance, Recognition and Recovery. In our approach, the possible attacks (faults and accidents) are divided into sub-events and then we calculate how the system responds to those events in resisting, recognizing and recovering from these events.

