Probabilistic Validation of Computer System Survivability*

William H. Sanders

Donald Biggar Willett Professor of Engineering,
Dept. of Electrical and Computer Engineering,
Coordinated Science Laboratory and Information Trust Institute,
University of Illinois at Urbana-Champaign, USA
whs@uiuc.edu

There is a growing need for systems whose survivability in a specified use and/or attack environment can be assured with confidence. Many techniques have been proposed to validate individual components (e.g., formal methods) or a system as a whole (e.g., red teaming). However, no single technique can provide the breadth of evidence needed to validate a system with respect to high-level survivability requirements. To accomplish this, we propose an integrated validation procedure (IVP) that begins with the formulation of a specific survivability requirement R and determines whether a system is valid with respect to R. The IVP employs a top-down approach that methodically breaks the task of validation into manageable tasks, and for each task, applies techniques best suited to its accomplishment. These efforts can be largely independent, and the results, which complement and supplement each other, are integrated to provide a convincing assurance argument. We then illustrate the IVP by applying it to an intrusion-tolerant information system being developed by the U.S. Department of Defense. In addition to validating the system against high-level survivability requirements, we demonstrate the use of model-based validation techniques, as a part of the overall validation procedure, to guide the system's design by exploring different configurations and evaluating tradeoffs.

* This is joint work with Sankalp Singh, Adnan Agbaria, Fabrice Stevens, Tod Courtney, John F. Meyer, Partha Pal, and the rest of the DPASA project team. The author is grateful for this collaboration.