Secure and Survivable Software Systems

Axel W. Krings and Paul Oman
Computer Science Department
University of Idaho
{krings,oman}@cs.uidaho.edu

With malicious computer and network attacks reaching epidemic proportions, issues of security and survivability of software systems have surfaced in a variety of application domains. Of real concern is the increasing reliance of critical applications on networked computer systems. Failure or compromises of such systems could cause threats to national infrastructures or lead to catastrophe (e.g., loss of life, damage to the environment, or unacceptable financial losses).

Driven by market speed and feature demand, commercial software developers have high pressures to deliver products rapidly, usually at the expense of quality and security. Given these market pressures and the increasing complexity of today's software, it is unrealistic to assume total security and robustness. Hence, the research area of secure and survivable systems has addressed the ability of systems to fulfill their missions even in the presence of failures, accidents or malicious attacks. Whereas resilience to failures and accidents has been the focus of research in fault-tolerant systems design, resilience to malicious attacks has become a challenge in the field of system survivability. Principally, essential services must be designed to withstand attacks. This requirement goes beyond the scope of computer and network security, which has been traditionally addressing detection and resistance to attacks.

When looking at survivable systems in general, the key assumption is that "anything is possible." One therefore should assume that intrusions will occur sooner or later. Considering the affects of intrusions, one has to recognize that in a computer any mechanism that empowers can (and will) be used against you (e.g., root or administrator privileges). This is different from fault-tolerance, where software and hardware design considerations address dependability issues such as aging of components, system environment, or electrical interference. Assumptions are typically made about the statistical probabilities of certain events. For example, it might be assumed much more likely for a component to fail in a safe state rather than fail in a specific asymmetric way causing pathological behavior. However, in survivability, the statistical assumptions do not hold. Attacks are assumed to be malicious rather than benign, and the probability of an attack does not necessarily follow predictable patterns. For example, if a vulnerability has been found in a specific system, but has not been published anywhere, the probability of this system being successfully attacked using the vulnerability is probably very small. However, posting the system's vulnerability in "hacker news groups" will almost certainly result in a successful attack.

In product development, design and test efforts have been traditionally motivated by the probability of faults. Metric fault models, Probability Risk Assessments, Fault-tree models, and hybrid fault models are all tools to model and increase reliability. However, as seen in the attack example above, it is extremely difficult if not impossible, to predict malicious behavior in open systems. As a result it may be difficult or impossible to predict which portion(s) of software systems are most vulnerable. Further compounding the problem are the economic and performance aspects like Automation, Efficiency, Transparency, Scalability, Maintainability, Responsiveness and Measurability, that cannot be overlooked when designing or modifying software for increased security or survivability. As a result, the task of identifying and designing solutions to increase software system security and survivability is a difficult research problem, requiring much attention by many researchers from a variety of perspectives.

The focus of this minitrack is on research that addresses the recognition and recovery aspects of software systems under malicious attack. The session will start with a forum on security and survivability initiatives at the U.S. National Institute of Standards and Technology (NIST), and then continue with five technical papers describing ongoing research efforts addressing the security and survivability of software systems used in critical areas. The papers in this minitrack cover a variety of different aspects of security and survivability, including failure modeling, attack recognition, and recovery from malicious acts at different software system levels.