Security and Survivability of Networked Systems

Axel Krings[*]
ID-IMAG
Montbonnot, France
axel.krings@imag.fr

Paul Oman
Computer Science Dept.
University of Idaho, USA
oman@cs.uidaho.edu

Azad Azadmanesh
Computer Science Dept.
Univ. of Nebraska - Omaha, USA
azad@unomaha.edu

The rate of adaptation of networked computers to control many aspects of our daily lives has continued the upward trend of recent years. In general, we seem to be quite comfortable to use computers to remotely access and manage bank and stock accounts, store financial and confidential data on diverse systems and even control our critical infrastructures. At the same time, public awareness of security problems is growing and increasingly more people understand the implications of their computers and applications operating in the unbounded environment of the global information grid. While it is unclear exactly how visible and vulnerable our systems and communications are, we must assume that increased visibility will result in the increased likelihood of cyber intrusion and/or attack.

Threats posed by viruses and denial of service attacks have been addressed in the general news media and by extensive advertisements by vendors and ISPs selling virus protection, spam filters and firewalls. The need for operating system maintenance, e.g. installing updates and security patches, is generally acknowledged, but the diligence of the system administrators is still far from perfect. Even the awareness of vulnerabilities of our critical infrastructures to Cyber attacks is growing, according to documentaries like PBS's *Frontline* expose entitled "Blackout"[1]. However, if one considers the fact that the registered number of malicious cyber incidents has almost doubled every year (CERT reported 137,529 incidents and 3784 vulnerabilities in 2003 alone[2]), the trust we place in our networked computer systems seems questionable and worrisome.

When dealing with the realities of cyber attacks, we tend to take the simplistic view of differentiating two system states, i.e. uncompromised or compromised. With respect to the first state, we apply methods that can be generally categorized as resistance strategies, whereas the current main strategy to deal with the second state is to detect or recognize the attack, largely ignoring recovery from the attack. However, not all functionalities of computers or applications we rely on have the same criticality. Whereas some services are essential to the very mission of the application, others may be suspended temporarily or their loss simply tolerated during an attack. Hence, survivability considers the behavior exhibited in the compromised state to recover the essential functionalities as an integral part of the application requirements.

Whereas fault tolerance is concerned with unintentional faults in software or hardware and provides solutions based on the statistical assumptions of the fault models considered, malicious behavior must be considered as an orchestrated, deliberate attack. Hence, the standard assumptions of fault tolerance do not generally apply in network security. To model and cope with cyber attacks we need to view the problem as a composition of security mechanisms for the resistance and detection aspects, and fault-tolerance methods with a new view of statistical realities for recovery. The general survivability model of resistance, recognition, recovery and adaptation was originally proposed by Ellison et.al.[3], and has since been embraced by the community of researchers working in systems survivability.

Even with the best intentions, the realities of survivable systems design impose a balance of cost and acceptable levels of risk[4]. This is especially true for safety critical systems, where failure can result in loss of life, property and environmental damage, but it is also true for non-safety critical systems where survivability is important for economics and continuity of service.

This minitrack is organized as a research forum to pursue the interrelationships between security, survivability, and dependability in large, non-trivial networked computer systems. Six research papers are included in two sessions that cover diverse issues showcasing recent progress in the security, survivability, and dependability research communities. The acceptance rate of the papers in this minitrack was 55%.

[*] The author is on sabbatical from the Computer Science Department of the University of Idaho with support from the Region Rhône-Alpes Ragtime project.

[1] PBS Frontline, "Blackout: What caused the power crisis in California? And who's profiting?," www.pbs.org/wgbh/pages/frontline/shows/blackout/, 2004.

[2] Carnegie Mellon University, Software Engineering Institute, CERT, www.cert.org/stats, 2004.

[3] R. Ellison, D. Fisher, R.. Linger, H. Lipson, T. Longstaff, & N. Mead, *Survivable Network Systems: An Emerging Discipline*, CMU/SEI-97-TR-013, 1997.

[4] W. R. Dunn, "Designing Safety Critical Computer Systems," *IEEE Computer*, pp. 40-46, Nov. 2003.