

Security and Survivability of Networked Systems

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

Before the success of the Internet, computer networks were generally designed for a well-bounded environment and defined audience. System users were limited to a known group with authenticated access, and intruders needed to physically penetrate a security perimeter before gaining access to the system. As a result, the main system security concern was guarding against insider abuse¹. Today, however, network applications are used in distributed, often malicious, environments where user characteristics, intentions, and backgrounds are largely unknown. In this unprotected setting, system vulnerabilities invite misuse, intrusion, and other forms of cyber attack. Data from Mitre's Common Vulnerabilities and Exposures (CVE) database² and CMU's CERT initiative³ shows that computer network security incidents and intrusions have grown almost exponentially over the last ten years. This epidemic of cyber attacks, coupled with the events of September 11, 2001, has demonstrated the need for more secure and survivable networked systems, especially those involved with critical infrastructures such as energy and transportation. Failure or security compromises in such systems may lead to catastrophic losses in lives, property, and the environment.

Unfortunately, 100 percent security is impossible to attain. Fortunately, we have recently gained an appreciation for the importance of survivability as a symbiotic partner to security. Furthermore, due to the pioneering work of Ellison et al., we now have a framework for studying aspects of network survivability⁴. *Survivability* is the capability of a system to fulfill its mission, in a timely manner, in the presence of attacks, failures, or accidents. This means that our control networks should be designed and operated so that essential services will survive even in the presence of malicious faults, intrusions, and attacks. Further, a system designed for survivability will maintain safe operations as long as possible, and in the end fail in a predefined safe mode of operation. Note that this definition goes beyond the traditional scope of computer and network security, per se.

According to Ellison et al., a secure and survivable computer network has the functional properties of *Resistance*, *Recognition*, *Recovery*, and *Adaptation*. Resistance and recognition address strategies for preventing, repelling and recognizing attacks. These are your traditional security functions. Recovery

encompasses those features that go beyond traditional security topics and directly focus on survivability. Adaptation refers to an evolution or reconfiguration based on knowledge gained from the malicious act.

When analyzing survivable systems in malicious environments the key assumption to hold is that everything is possible, but the probability of an event occurring is not a static function. This is different from fault-tolerance, where software and hardware design addresses dependability based on issues like component aging, benign failure rates or phenomenal interference. Assumptions are made about the statistical probabilities of these events. In survivability, these statistical assumptions do not necessarily hold. Attacks are assumed to be malicious rather than benign, and the probability of an attack does not follow predictable patterns. For example, if a system vulnerability has not been disclosed, the probability of the system being attacked through that vulnerability is small. However, once the system's vulnerability is publicly disclosed (e.g., posted to a hacker news group), there will almost certainly be an attack.

This minitrack was organized as a research forum to pursue the interrelationships between security, survivability, and reliability in large, non-trivial, networked computer systems. The papers are divided into two sessions, separated by a presentation on *Security Trends and Initiatives at the U.S. National Institute of Standards and Technology* (NIST). The three papers in the first session address ways of measuring and testing security properties in software systems. The NIST presentation provides a forum for learning about some of the U.S. government's security and survivability research initiatives. In the last paper session, we have combined a paper on ad-hoc sensor networks with two papers from the minitrack on *Secure and Survivable Mobile Agents*.

¹ J. Allen, A. Christie, W. Fithen, J. McHugh, J. Pickel & E. Stoner, *State of the Practice of Intrusion Detection Technologies*, CMU/SEI-99-TR-028, ESC-99-028, 2000.

² Mitre, Common Vulnerabilities and Exposures, www.cve.mitre.org/about, 2003.

³ Carnegie Mellon University, Software Engineering Institute, CERT, www.cert.org, 2003.

⁴ R. Ellison, D. Fisher, R. Linger, H. Lipson, T. Longstaff, & N. Mead, *Survivable Network Systems: An Emerging Discipline*, CMU/SEI-97-TR-013, 1997.