



# DEFENSIVE INFORMATION WARFARE

• BRAJENDRA PANDA AND JOSEPH GIORDANO,  
GUEST EDITORS

As the wonders of global connectivity unfold, the world is changing its perception toward the use of computers. Computers are no longer viewed as mere number-crunching devices nor is the use of computers limited to the scientific and engineering communities. The advent of high-speed networking technologies has made information sharing through the Internet a prevailing practice for every conceivable segment of society from governments to business and industry to private citizens.

Every day, millions of people use the Internet to search for different kinds of information stored in computers and databases that may be on the other side of town or half a world away. While most of these users access data legitimately, some use illicit ways to access and invade other computers. It is extremely hard to protect systems from all types of unauthorized access. Sophisticated hackers and crackers work diligently to find security loopholes and use these loopholes to break into systems. Besides attacks from outsiders over the network,

there remains the possibility of an invasion of one's system by an insider turned foe. Any such malicious attack against an organization's information base through electronic means is termed *information warfare*. Such an attack may be intended to cause temporary turmoil in the operations of the organization including denial of service, or even to cause extensive damage to the organizational information infrastructure. One only has to read the newspaper or watch the nightly news to see how the concept of information warfare has emerged from the arcane world of

research laboratories to become an issue of major concern to every segment of the population. As stated in the report of the President's Commission on Critical Infrastructure Protection,<sup>1</sup> information technology is a key component of the fabric of the critical infrastructure of the U.S. The public telephone network, banking and finance, vital human services, and other critical infrastructures are dependent upon information technology for their day-to-day operation and must be adequately protected.

The objective of defensive information warfare ranges from ensuring authorized use of computer resources to providing complete, uninterrupted operation of computer systems throughout all of the phases of an information attack. A functional paradigm of defensive information warfare is best described by the following actions: *protect*, *detect*, and *react*.

Protection techniques must be designed to guard hardware, software, and user data against threats from both outsiders as well as from malicious insiders. This involves simple mechanisms such as development of rules for users including password management to sophisticated access control and integrity mechanisms. These protection techniques must be designed keeping risk management in mind. Risk management implies the balancing of information technology vulnerabilities against the perceived threat's ability to exploit these weaknesses. Simply stated, an organization can't protect everything—trying to protect everything is the same as protecting nothing. In this section we have included two articles related to information protection mechanisms. The article by Shiu-Kai Chin proposes formal methods for verifying the security strengths of computer systems. Anup Ghosh and Jeffrey Voas present an approach that helps build robust systems by introducing errors and then testing the fallibility of the system in order to improve system immunity.

The ability to quickly and correctly detect and identify malicious information attacks is critical to the survival (meaning the uninterrupted operation) of information systems. Regardless of strong protective measures, it is difficult to repair all security vulnerabilities in distributed and networked computing environments. For example, a user may take a risk that may be unacceptable to others who share the same network. The security of the entire system, like a chain, is only as strong as the weakest link. The realization that the protection can never be comprehensive makes it necessary to be vigilant in reporting any suspicious activities that may indicate an attack. If an

information attack takes place, the victim must have the capability to degrade gracefully and recover damaged data or services in real time. Detection and identification of attacks is especially difficult when the adversary is sophisticated and launches a well-organized, subtle, distributed, coordinated information attack. Successful detection of intrusions and misuse can be achieved only by gaining an accurate understanding of the "state" of the system at any given point in time. With that in mind, several articles on intrusion detection mechanisms appear in this section. Terrance Goan addresses issues concerning false alarms raised by intrusion detection systems and ways to improve the performance of these systems. While Robert Durst and coauthors discuss intrusion detection mechanisms and procedures for evaluating their effectiveness, Matthew Stillerman and coauthors apply the intrusion detection technique to a distributed CORBA-based environment.

The post-intrusion detection process is concerned with assessing damage, finding malicious hidden programs, locating and closing any back doors left by an attacker for future reentry, and recovering data. These activities are spawning an emerging field called computer and information system forensics. Computer and information system forensics is concerned with a continuum of activities including the collection of audit and intrusion detection data, analysis and interpretation of that data, and evidence reconstruction for legal purposes. Quick and complete recovery of the system after an attack is undoubtedly vital for successful and continued operation of any organization. It is crucial to maintain the system integrity and availability during the repair of the damage inflicted by the information attack. The article by Sushil Jajodia and coauthors focuses on the damage assessment and recovery framework, discussing several methods that can be used based on the attack characteristics and the severity of the damage.

Defensive information warfare will remain an active research and development area for years to come as new technologies emerge and the cat and mouse game between attackers and protectors continues. We hope the articles presented in this section will promote better awareness among readers regarding various problems and techniques available for defending their computing resources. **C**

---

**BRAJENDRA PANDA** (panda@cs.und.edu) is an assistant professor of Computer Science at the University of North Dakota.  **JOSEPH GIORDANO** (giordanoj@rl.af.mil) is the technical advisor for the Defensive Information Warfare branch of the U.S. Air Force Research Laboratory, Rome Research Site, Rome, NY.

---

<sup>1</sup>*Critical Foundations: Protecting America's Infrastructure*. The Report of the President's Commission on Critical Infrastructure Protection, October 1997.