If history is any indication, the information technology community is incapable of constructing networked information systems that prevent unauthorized intrusions and abuse. Even organizations that take computer security seriously remain susceptible to attacks of many forms, as has been demonstrated by several significant penetrations into U.S. Department of Defense (DoD) computers. Denning relays an account of hackers from the Netherlands who penetrated 34 American military sites on the Internet, including military supply systems, that were supporting Operation Desert Storm. Between April 1990 and May 1991, the attackers gained information about the exact locations of U.S. troops, their weapons, and the movements of U.S. warships. They even gained the ability to manipulate military supply systems, and to change what supplies were shipped to what locations. More recently, this year DoD computers have been the target of a focused attack—dubbed “Operation Moonlight Maze”—originating from Russia. Publicly confirmed damage due to the attack has been significant.
VULNERABILITY OF NETWORKED SYSTEMS

Numerous factors contribute to the vulnerability of our networked information systems. First, the dramatic increase in network connectivity during this decade has enabled attacks to be conducted from a distance, across many administrative domains, and often anonymously.

Second, the state of software engineering practice, particularly with respect to software for Internet applications, largely ignores issues of assurance. Most software today is "assured" by the penetrate-and-patch approach—when someone finds a vulnerability, the software manufacturer issues a patch. This approach has proved inadequate but is economically attractive for the manufacturer. When such software is executed on the same system with other software similarly "assured," further vulnerabilities can be introduced.

Third, poor administration practices and tools can result in a system remaining susceptible to vulnerabilities even after appropriate patches have been issued, and can introduce additional vulnerabilities into what would be an otherwise relatively secure system.

Lastly, even a system that has been well hardened to outside attack can be undermined by a legitimate user through operational errors or intentional manipulation. Since there is little reason to believe that these factors will be eliminated in the near future, we need to rethink how we build networked information systems.

PROTECTING CRITICAL SERVICES

Survivability has emerged as a new requirement for these systems. The term "survivable" refers to distributed architectures that can continue to meet application requirements despite successful penetrations into component computers. Survivability is an especially important requirement given that increasingly critical applications are being migrated to interconnected networks. Examples include the computers that run the U.S. electric power grid and some 911 telephone systems, both of which were found in a 1997 exercise by the National Security Agency to be reachable from the Internet and vulnerable to attacks that could result in severe degradation.

Survivability is an issue at all technological levels of a networked information system. At the network level, where delivery of packets to their intended destination is the service to be preserved, survivability may involve redundant routing of network packets to the destination via multiple disjoint routes. In this way, an attacker that overtakes a network router cannot prevent the packets from reaching their destination. Above the network level, a distributed storage facility might employ redundant storage to detect or mask the manipulation of individual data stores. Cryptographic techniques can further be employed to prevent the disclosure of sensitive data when a component is penetrated.

Survivability

Protecting Your Critical Systems

Robert J. Ellison, David A. Fisher, Richard C. Linger, Howard F. Lipson, Thomas A. Longstaff, and Nancy R. Mead

Survivability is the capability of a system to fulfill its mission in a timely manner in the presence of attacks, failures, or accidents. Key to the concept is the identification of essential services, and the essential properties that support them, within an operational system. Survivability focuses on unbounded networked systems, such as the Internet, where traditional security measures are inadequate. As an emerging discipline, it builds on related fields of study (such as security, fault tolerance, reliability, and verification) and introduces new concepts and principles.

Building Trustworthy Systems: Lessons from the PTN and Internet

Fred B. Schneider, Steven M. Bellovin, and Alan S. Inouye

The Public Telephone Network and the Internet are both likely to furnish communications services for most other Networked Information Systems that require a global infrastructure. Leaders of the U.S. National Research Council’s study committee on information systems trustworthiness describe vulnerabilities in these two large, complex, and in some ways very similar networks. The authors report a “trust gap” emerging between the needs and expectations of the public and the capabilities of today’s NISs and, more troubling, a lack in the science and technology base to build trustworthy NISs.

Such techniques generally must be coupled with intrusion detection capabilities to monitor for attacks, response capabilities to stem the attack once detected, and a recovery strategy to repair damage. Throughout these operations, the critical services provided by the system must remain available and correct.

FRAMING THE ISSUES

This special section contains two articles that shed greater light on the issue of survivability. The first, “Survivability: Protecting Your Critical Systems,” by Robert J. Ellison et al. at CERT (pp. 55-63), provides background on the concept of survivability and a glossary of terms, and outlines work
Interested in being an IC reviewer?

IEEE Internet Computing seeks referees for submissions on Internet technologies. Please send your name, contact information, short curriculum vita, and keywords for your areas of expertise (see the list at http://computer.org/internet/xtras/index.htm) to magazine assistant, Hazel Kosky, at hkosky@computer.org.