

The National Strategy to Secure Cyberspace

Higher education has been involved in the computer security business from the first time that grades and paychecks were stored in a campus mainframe. Since then, exposure has grown by magnitudes as college and university systems have been entrusted with personal and professional information, credit card numbers and financial transactions, data for research in progress, patented and copyrighted intellectual property of all types, private communications, and even medical records. The normal functioning of higher education institutions now absolutely depends on secure and private access to this information. Yet until recently, campus computing security remained a campus concern: national security considerations for computing at colleges and universities were limited to a small number of specialized labs.

This situation changed with the invention of a simple, but hard to stop, threat called a distributed denial of service (DDOS) attack. In a DDOS attack, hundreds or thousands of computers are programmed to send messages over the Internet at the same time, all to the same recipient computer. The resulting flood of information becomes too much for the victim computer to handle, with the result that it can no longer respond to legitimate requests during this timeframe, effectively denying its services to the world. It is as if thousands of your "friends" conspired to each call your telephone number over and over, rendering your phone permanently busy and unavailable. In more innocent circumstances, this is what may happen by accident when all the long-distance lines from a city are busy on Mother's Day.

A DDOS attack is much more dangerous for computer systems, however, because a lone hacker can enlist the services of thousands of computers that are owned and operated by others and usually can do so without their knowledge. The hacker uses automated tools to scan every computer on a network, looking for security vulnerabilities such as easy-to-guess passwords, known security flaws that have not been "patched," or other means of entry. Once inside, the hacker takes command and may modify or steal private information or install malicious programs, generally leaving no visible trace of the crime.

Such online scans for "holes" in security now occur relentlessly, day and night, on virtually every system connected to the Internet. Campuses of all types and sizes are an especially tempting target because they operate so many computers on such fast networks and because many of their computers (e.g., those owned by students) have little professional management. One prominent research university estimates that every networked computer on campus is scanned for vulnerabilities at least twice a day, that a new computer plugged into the network is scanned within minutes, and that if vulnerabilities are found, a computer is compromised by intruders within an hour. Network engineers on the largest research network in the United States measure up to twenty "high alerts," or significant periods of DDOS-like attacks, on a daily basis.

Campus computers have been implicated in several major DDOS attacks on important installations in government and e-commerce. For this reason, higher education is sometimes said to pose a threat to others and even to national security, fur-

ther raising the stakes in the battle to make campus computers more secure. Helping colleges understand the problem and work together on effective solutions is a focus of the EDUCAUSE/Internet2 Computer and Network Security Task Force (<http://www.educause.edu/security>), created in July 2000. The issues addressed by the task force rose in importance after September 11, 2001, culminating in an effort by the President's Critical Infrastructure Protection Board (PCIPB) to lead the development of a National Strategy to Secure Cyberspace. The result is a national strategy, not a government strategy, since most of cyberspace is owned by the private sector (and much is owned by higher education). The strategy calls for every sector to take appropriate actions to secure its own portion of cyberspace, since all parts depend on each other and attacks can be launched on all from the weakest links.

The EDUCAUSE/Internet2 Computer and Network Security Task Force has worked closely with the PCIPB and member institutions to develop the higher education contribution to the National Strategy to Secure Cyberspace. It is now working to translate the strategy into a plan with concrete actions that can be used to secure computers and information on campuses of all types. Higher education must protect its own critical information, for the usual important reasons. But higher education must also work to better secure *all* of its systems in order to become part of the solution, not part of the problem, with respect to DDOS and other cyber threats to the Internet, the economy, and the national security.

Mark A. Luker is Vice President of EDUCAUSE.