

“Free Love” and Secured Services

Approximately three years ago, Columbia University became an exception to conventional network-security wisdom: it made the bold decision to stop registering computers on its network unless they needed a fixed name. This new scheme, fondly called “free love,” allowed all computers—public or private; wired or wireless; in residence halls, at the libraries, in faculty and staff offices, or anywhere else on campus—to connect directly to the network, and thereby to the world, without further ado. The Academic Information Systems (AcIS) staff, who manage the campus network and its connections to the outside world, did not embrace this decision unanimously. Many thought it would be a giant backward step in managing security. Yet three years into the experiment with free love, the decision has proven to be successful not only for the users, who gained convenience, but also for the AcIS staff and for management.

One of AcIS’s self-serving reasons for implementing this new policy was to stop being the bottleneck in the process by which new students, staff, and faculty connected to the network. Previously, AcIS had annoyed its customers, since its bureaucratic desire to register their computers delayed the productive start of their tenure at Columbia. So much frustration! So much cost! So little benefit! And what about visiting scholars or guest lecturers? How much time and effort had been expended by the office of a dean or department chair to obtain and register the Ethernet address of a visitor’s laptop? Visitors too could now get on the network without divine intervention and could

get their work done without waiting “up to ten business days,” as the AcIS registration instructions had warned them in the past.

Columbia had never charged users for networking based on registration. Therefore, there were no business reasons to continue the practice. In addition, registration alone never prevented any security breach or abuse. After all, network addresses, easily spoofed, have never been good links by themselves in a chain of evidence. For proof that someone with an Ethernet card has committed a crime, the evidence needs to show that the Ethernet address accessed networked resources that required a log-in with a personal ID and password before and after the crime. Bingo! If the use of passwords to access services is the key to proving abuse, why should the members of the user community be required to register when they show up on campus? Access to services can be tracked by keeping good logs (in DHCP servers and those applications that require log-in, such as e-mail and course-management systems) and by implementing policies and systems that keep IDs and passwords private. Registration adds nothing if access to services can be tracked.



Illustration by Steve McCracken, © 2002

The network is the swamp. Security belongs in the applications—the islands and solid ground of the swamp—not in the network itself. Security, in other words, is an issue for those who manage services and hosts. Without appropriate authentication and authorization in applications, information resources cannot be secured against abuse. If the network is the security perimeter, unauthorized access or security infringements will always occur, because the criminals are always one step ahead of those who try to secure the swamp. They always find the weakest link on campuses, usually a de-

partmental server or someone's overactive and undersecured desktop, and launch their attacks from there, pretending to be authorized network users.

Some might argue that not registering networked computers carries costs of its own. But what are those costs? What exactly is an institution protecting by policing who gets on to its network? Others might argue that without some control over network access, an institution will be giving away free bandwidth. But what is the impact of this bandwidth "loss"? How does it compare with the loss of bandwidth caused by all those users who are legitimately connected and are performing illegal file-sharing or allowing denial-of-service attacks to be launched from their servers? For that matter, how does it compare with the loss of bandwidth caused by incoming spam messages? An institution is better off investing in technical development focused on security and performance for its services than investing in relatively inefficient and ineffective network security.

It's not as though Columbia ignores the security of its network. Unusual network utilization, Klez, Code Red, and spam activity are monitored continuously. Specific machines on the wireless and wired network are blacklisted, if necessary, using their Ethernet hardware addresses. Naturally AcIS security staff, who respond to security incidents and especially to law-enforcement requests, wish there were easier mechanisms to extract appropriate logged network data. Yet the majority of this work involves information that has nothing to do with registering machines on the network. In any case, it is not clear that network registration delivers the biggest security bang for the technology buck.

Network registration is an expensive half-solution. For example, forcing Ethernet address registration does not eliminate concerns related to the Health Insurance Portability and Accountability Act (HIPAA); these can be handled by properly employing host-based encryption technology. As long as a campus network swamp is connected to the Internet swamp, its applications and data are only as secure as the applications themselves: unless the authentication, authorization, and encryption built into applications

are trustworthy, the applications are vulnerable.

Columbia employs Kerberos authentication as universally as possible. It has over 250,000 University Network IDs (UNIs) in its system, all of which have appropriate authorization levels defined in a central directory. Indeed, this directory is used to operate Columbia's modem pools, and yes, I admit that access to the network from modems is secured, but only because modem access is a scarce resource. Secure web servers implement access to restricted or licensed library resources, administrative systems, e-mail, and the course-management system. Secure e-mail is encouraged through mail services whose interactions employ SSL encryption, and outgoing mail servers require encryption and authentication. Antivirus software is provided free to every member of the university community. Filters for detecting virus and worm infections such as Klez and Code Red are in place centrally. The incoming mail servers have virus breakers, as well as spam detectors. Encrypted and secure telnet sessions are used. These are the appropriate choices to combat the "bad guys," rather than making the user community jump through hoops for the sake of administrative processes.

In the future, all this might change. Change might be driven by a business need to identify machines, as opposed to users, on the network. Even then, our solution would be to implement a network log-in mechanism to identify the network appliances rather than to reinstate hardware registration. We might also reconsider our current policy if network authentication could be implemented universally, using open standards, with systems based on scalable and transparent technology rather than network trickery, and only if we could implement a responsive UNI-creation technique that requires much less bureaucracy than it does now. But none of these scenarios seem likely in the near future, so for the moment, free love lives on in Morningside Heights.

Vace Kundakci is Deputy Vice President, Academic Information Systems, at Columbia University.



EDUCAUSE

Transforming Education Through Information Technologies

EDUCAUSE, a consolidation in 1998 of Educom and CAUSE, is a nonprofit consortium of colleges, universities, and other organizations, dedicated to the transformation of higher education through the application of information technologies. Through direct services and cooperative efforts, EDUCAUSE assists its members and provides leadership for addressing critical issues about the role of information technology in higher education.

EDUCAUSE Board of Directors

Martin D. Ringle, Chair
President, NorthWest Academic Computing Consortium
Reed College

Amelia A. Tynan, Vice Chair
CIO and Vice Provost
University of Rochester

Joanne R. Hugi, Secretary
Associate Vice President,
Information Services
University of Oregon

Joel L. Hartman, Treasurer
Vice Provost, Information Technologies and Resources
University of Central Florida

Kathleen Christoph
Director, DoIT Academic Technology Solutions
University of Wisconsin-Madison

Perry O. Hanson III
CIO and Associate Provost for Educational Technology
Brandeis University

Gregory A. Jackson
Vice President and CIO
University of Chicago

Joel W. Meyerson
Director
Forum for the Future of Higher Education

Susan L. Perry
Senior Advisor, Andrew W. Mellon Foundation
Mount Holyoke College

William H. Pritchard
Vice Chancellor and Chief Technology Officer
Foothill-DeAnza Community College District

Steven W. Relyea
Vice Chancellor, Business Affairs
University of California, San Diego

David Ward
President
American Council on Education

Ex Officio Member
Brian L. Hawkins
President
EDUCAUSE