ANONYMITY: WE WANT IT AND WE DON’T. We need and want to share our stories, but we also want the details of our lives to remain in our personal control—to release them if and when we decide the time is right, for reasons we determine are worth the loss of a degree of privacy.

As technology expands the way we operate in the electronic environments of colleges and universities—and provides us with new tools for teaching, learning, and research—important ethical issues concerning privacy arise. In this rapidly changing environment, we rarely have the opportunity for in-depth discussion of the different viewpoints on such issues. The push to efficiency, to rapid change, and to application of new technologies often causes key and extremely important issues to be glossed over.

One such issue is whether to require authentication for a user to access electronic resources within a campus environment. Somewhere along the continuum from total security to open access lies a viable path, but getting to that path is not easy. The issue calls for extensive debate, since the questions surrounding resource access in libraries are many and complex. Are incidents of abuse currently happening through or on library networks? What responsibilities and obligations do library professionals have to their users? What responsibilities and obligations do security professionals have to their users? (Sometimes these two groups of users overlap.) What resources in the library are on the networks? How does access to library resources differ from access to other resources on-site?
or elsewhere on campus? What are the risks if authenticated access is required? What are the risks if unauthenticated access is allowed?

These questions offer potential for conflict at multiple levels in this debate. At the most basic level are different responsibilities, different values, and distrust. As we move on to process, different experiences and different language come into play. Once we reach action steps, logistics and the unknowns of technology add to the tension. Different opinions about alternatives bring the conflict to the table. The worst scenario is a rush to resolution, causing theままiming of the values and standards of one group for the sake of closure and expedience. This can leave a campus without coherence and the required cooperation.

Different Responsibilities, Different Values, and Distrust

Librarians have long been among the staunchest defenders of First Amendment rights. They care deeply about, and feel responsible for, protecting user privacy and freedom of expression. They understand the importance that information access plays in a free society. However, as part of the increased emphasis on free access, there is a fear that networks may become a source of an abuse and who was using the source machine at the time. They are not interested in who a particular individual was accessing or reading when an attack was committed.

Once authentication logs are maintained, however, both groups agree that the ability to draw conclusions about the services used by an individual may incriminate or exonerate the user against him or her, thus reducing the degree of freedom. Some library services are already tied to authentication, to protect resources against tampering, to ensure that networks are operating, and to maintain and protect systems. In that way, resources can be implemented as free of additional charge and made available to all.

Equity of Access

For librarians, “equity of access” means that there should be no restriction on who can access resources and that no one person, by virtue of privilege or experience, should have more access to public information than another person.
the low rate of abuses in the library, they conclude that librarians are unaware of the severity of the problem and not fully conscious of the security that they value so highly.

In addition, the different work environments of the two groups may add to this distrust. Psychologists such as Erik Erickson, Abraham Maslow, and many others have described the importance of consistency and predictability in life and how these factors lead to the development of trust. In our current information technology environment, and they are expected to manage more rapidly changing environments. Security professionals, however, have no such consistencies. Their newer, less established environment is more unstable and subject to change than the library environment, and they are expected to manage and respond to both. The rate of growth and the direction of new innovations are unpredictable and chaotic. There is a considerable difference between the more used, methodical approach of libraries and the experimental, risk-management approach of systems.

**Different Experiences and Different Language**

The different experiences and the resulting different language of these two groups have resulted in confusion and misunderstanding. One area of divergence involves the perception of resource abuse on the campus. Librarians perceive the percentage of abuses relative to the whole population to be low. They think that the community should not be given resources that are underprotected and that are subject to abuse, free access being chiseled away. When security professionals talk of nonreplaceable physical resources, they isolate the offender rather than rely on institutional facilities. All representatives of libraries feel comfortable with, or have experience with, security (protection against theft and destruction of, all users).

Incidents of inappropriate and abusive use—through Telnet, gateways, and e-mail—and threats to individuals and institutions happen from unauthenticated library machines. In a recent meeting of state universities and law enforcement personnel, representatives were asked for examples of electronic threats occurring on their campuses. The crux of the conflict between librarians and security professionals arises over the perception of resource abuse on the campus.

Librarians perceive the perception of resource abuse on the campus. Librarians perceive the percentage of abuses relative to the whole population to be low. They think that the community should not be given resources that are underprotected and that are subject to abuse, free access being chiseled away. When security professionals talk of nonreplaceable physical resources, they isolate the offender rather than rely on institutional facilities. All representatives of libraries feel comfortable with, or have experience with, security (protection against theft and destruction of, all users).

Incidents of inappropriate and abusive use—through Telnet, gateways, and e-mail—and threats to individuals and institutions happen from unauthenticated library machines. In a recent meeting of state universities and law enforcement personnel, representatives were asked for examples of electronic threats occurring on their campuses. The crux of the conflict between librarians and security professionals arises over the perception of resource abuse on the campus.

Librarians perceive the perception of resource abuse on the campus. Librarians perceive the percentage of abuses relative to the whole population to be low. They think that the community should not be given resources that are underprotected and that are subject to abuse, free access being chiseled away. When security professionals talk of nonreplaceable physical resources, they isolate the offender rather than rely on institutional facilities. All representatives of libraries feel comfortable with, or have experience with, security (protection against theft and destruction of, all users).
How can we provide that access technically?

How do we protect individual privacy?

How do we balance the needs for access to information (users), protection of information (creators), and cost recovery for providing information (publishers)?

How do we articulate a comprehensive and comprehensive policy that will enable us all to work?

How do we ensure good communication, the development of a common language, ongoing discussion that does not falter in moments of crisis, and a balanced policy that meets many diverse needs and values?

How do we deal with the authentication issue (1) at the network level and at the resource level, using login/password and guest passwords for noncommunity members (high barrier), (2) at the network level only (medium barrier), (3) at the resource level only (medium barrier), or (4) at no level, that is, no authentication (low barrier)?

To begin to decide what solutions would best balance the values and needs of these two groups of professionals, we should first sample incidents that occur from unauthenticated library computers. The next step is to gather statistics that show the volume of use of various services such as HTTP, SMTP, POP3, Telnet, and ftp. These data can help to identify services that could be removed from unauthenticated-access machines to reduce vulnerability. The final step is to examine the types of services offered in the traditional library environment and those offered in the electronic environment with a view to comparing the driving forces that lead to some form of protection for those resources and the nature of the protection that is currently being implemented. It is helpful to identify these protections in terms of the IAA components described earlier. These sources of information will help maintain a focus for critical discussions and policy development.

Regardless of the results of data analysis or debate, we all must understand the process and the issues. For any process to be successful, communication must be open and continuous. The parties involved must keep talking, keep listening, and keep questioning. This is particularly true when there are different responsibilities and values, distrust, different experiences and language, different logistics, and incomplete knowledge about technology.

Critical questions are yet to be answered. How do we reconcile the belief in freedom of information, freedom of access, freedom from monitoring and censorship, and protection of privacy with the need to maintain integrity of resources, protect individuals from unwanted and unwarranted intrusion, assure creators of information that their data will not be compromised, and ensure that the copyright belonging to creators and publishers of information is protected? Legally, how do we reconcile the varying requirements of FERPA (Family Educational Rights and Privacy Act), FOIA, Lending Records laws, Federal Depository obligations, copyright law, and the myriad laws that are now being created around the communications and computer industries? This, of course, presumes that we all agree about how those laws are interpreted, which is clearly not the case.

How do we create a policy in light of changing technology? What are the technical options, who understands them fully, what will come tomorrow, and how will we create any kind of strategy, direction, or lasting policy amid such change? How should we establish responsibility for content validity and reliability? What belongs to the institu-
How do we reconcile the belief in freedom of information, freedom of access, freedom from monitoring and censorship, and protection of privacy with the need to maintain integrity of resources, protect individuals from unwanted and unwarranted intrusion, assure creators of information that their data will not be compromised, and ensure that the copyright belonging to creators and publishers of information will be protected?

from unauthenticated library machines in order to reduce potential network vulnerabilities.

Conclusions

We would not have found the time to examine these issues so carefully had we not come to a near impasse in attempting to write policy about authentication for electronic resources on our own campus. In the midst of frustration, a mounting sense of urgency, intensely held but differing values, a sense of responsibility based on different perspectives, a lack of understanding of variant viewpoints, and a lack of knowledge about technical possibilities, we experienced a breakdown in communication, followed by an entrenchment in viewpoints. A full solution has not yet been found; however, the issues that emerged have expanded our understanding of underlying values and have broadened our appreciation for the professionalism and objectives of both librarians and security professionals.

There are clearly many questions and no easy answers. The opportunity for debate on this important ethical issue lies before us. The keys to success lie in maintaining balance and continuing discussions. Whatever happens, keep talking!

Notes


EDUCAUSE 2000

Converging/Emerging in the 21st Century

Nashville, Tennessee
October 10–13, 2000

The EDUCAUSE 2000 information technology conference is one of higher education’s preeminent educational events.

The annual EDUCAUSE conference attracts thousands of participants and attendees from institutions and corporations throughout the world. Last year we offered 32 preconference seminars, more than 150 track sessions, over 150 corporate exhibits, almost 100 poster sessions, and dozens of current issues sessions, constituent group meetings, and corporate presentations and workshops. Of course, we also offered our attendees innumerable opportunities to network with peers and vendors.

This year promises to be even better.

We hope you’ll join us as the best and the brightest gather in Nashville to chart the future of information technology in higher education. We know you’ll enjoy being part of the crowd that includes David Halberstam, journalist/author, and Dave Barry, syndicated columnist/author; two of our general session speakers.

Be sure to mark October 10–13, 2000, on your calendar and look for conference details on the EDUCAUSE Web site beginning in April.

www.educause.edu