

Digital Security in a Free Society

As a graduate student, I was in the Ph.D. program in history during the 1960s at the University of Wisconsin, Madison, where I studied under Allan Bogue, one of the pioneers in incorporating quantitative analysis and social science research methodology into the field of history. My dissertation and subsequent book focused on the politics of populism in Colorado in the nineteenth century and included an extensive statistical analysis of voting patterns. As part of my work, I learned to do Fortran programming and to wait patiently for batch processing. When I first arrived at Dartmouth College in 1969, I came with a stack of computer punch cards and entered an environment that was extremely computer-friendly.

John Kemeny, the coinventor of the BASIC computer language and formerly a math professor, became president of Dartmouth in 1970. He adopted a philosophy of complete computer access—computers were for everyone. He encouraged students and faculty from across the institution to experiment with and to use the new technologies available to them. In the thirty-plus years since that time, Dartmouth has moved from having mainframe computers and time-sharing, to implementing one of the first fully networked systems, to being the first completely wireless campus. Computers are now ubiquitous and play a critical, even central, role in the lives of Dartmouth students and faculty and add immeasurably to the learning and research environment.

In our society, as technology—computing, in particular—has become more integrated into our daily lives, issues of

security have become paramount. Highly confidential personal information, legal documents, commercial transactions, and many other materials are transmitted daily over the information highway. In addition, within the academic community, data sets, preliminary research findings, and sensitive research proposals are transmitted across campuses and, indeed, across the world. As institutions of higher learning, colleges and universities have a responsibility to facilitate communication and sharing while also contributing to the creation of new safeguards. The need to protect information has become one of the most difficult problems facing higher education institutions. Faculty must play a role in the discussions and debates revolving around the standards and protocols that govern who has access to what information. It is this last issue that is perhaps the most difficult as educational institutions seek to balance a commitment to openness and access with a need for security and oversight.

In 2001 Dartmouth, working with the U.S. Justice Department's National Institute of Justice, opened the Institute for Security Technology Studies (ISTS) and participated in the testing and development of a new Public Key Infrastructure. ISTS is a national center that focuses on cybersecurity and counterterrorism technology research. The Institute studies threats to the electronic information infrastructure systems and technologies of the United States, seeks appropriate and effective responses, and assesses training and information needs. Such research is of vital importance to the nation's security interests and has implications for the commercial and academic realms.

The Public Key Infrastructure (PKI) project focuses on the day-to-day security needs of the higher education institution. This project is sponsored by the Internet2 consortium, which has named Dartmouth and the University of Wisconsin, Madison, as the two sites to host a PKI Lab to work with government and industry on public key cryptography. Although public keys already exist on many campuses, this project will help to develop much-needed protocols and standards for the use of such keys.

Public key systems enable parties to engage in the trusted exchange of information even if they have never met and share no secrets beforehand. Such systems help to address the basic problems of digital security:

- **Authentication:** Are you who you say you are?
- **Authorization:** What are you allowed to do or access?
- **Protection:** Can I be sure that if you intercept my information, you won't be able to decipher it?
- **Information Integrity:** Can we be assured that what I sent is exactly what you received?
- **Private Channels:** Can we open a communication channel that others can't access, and can we assure ourselves as to the integrity of what we send on that channel?

The need for greater digital security plays out in three areas of academic life. Perhaps the easiest to describe is the administrative realm. The ability to render business processes paperless holds enormous economic and bureaucratic appeal.

Think about the benefits of paperless but secure and signed processing of hourly time sheets, payroll actions, sponsored research administration, and student information such as billing and grades. Other administrative examples abound. And there is a need to use these techniques in communication and information transfer between institutions. The PKI bridge experiment between higher education and the federal government in January 2002 demonstrated an approach for meeting this need.

A second area where public key systems could be invaluable is in protecting

working with a number of higher education institutions—as well as with Internet2, EDUCAUSE, and the Southeastern Universities Research Association—to develop “middleware,” or advanced network software, that is simple to use, broadly available, and secure.

A third role for digital security within the academy relates to scholarly content. An incredible amount of scholarly material is now available online, and much new scholarly work is published in a digital format. The digital world is fast replacing print as the medium for the provision of information. Two vital scholarly content

digital world. Digital content has changed the work of publishers and libraries and has had profound effects on authors as well as subscribers. Many questions remain. Which parties will participate in the ownership of a particular instance of digital content? What form will that content take? What will be its boundaries in terms of provenance and future incarnations? How will access be controlled? How will payment for access take place when necessary? How can unauthorized “reproduction” be controlled?

Academics need to be integrally involved in finding the answers to these

questions. But as we confront these issues, and as we confront a world changed by terrorism, we need to be careful that we do not stray from the basic principles of access and openness that John Kemeny articulated and that the academy embraced so many years ago. Colleges and universities are not, by definition, secretive places. They thrive on the free exchange of ideas and on open debate. But nor can we afford to be Pollyannaish about the real changes that have occurred in the digital world in which we live and learn. Thus we must strive for a sensitive balance between openness and security, between access and control. We need both. And if we are to get both, and if we are to maintain the balance, we must ensure that academic institutions and faculty are well represented at the table as these issues are discussed and as protocols and standards are developed.



Illustration by Jung Hoang, © 2002

academic communications such as sensitive data used by researchers, time-stamped and authenticated submissions of assignments or articles, and authentication and authorization for collaborative work among students and faculty. The National Science Foundation is

issues related to security are intellectual property (IP) rights and copyright. In the digital world, these issues are generally referred to as Digital Rights Management, or DRM. DRM is critical for higher education. The management of rights in the print world does not translate easily to the

represented at the table as these issues are discussed and as protocols and standards are developed.

James Wright is President of Dartmouth College.

